Fortinet Auto Discovery VPN (ADVPN)

Stéphane HAMELIN – Escalation Engineer

01 July 2016

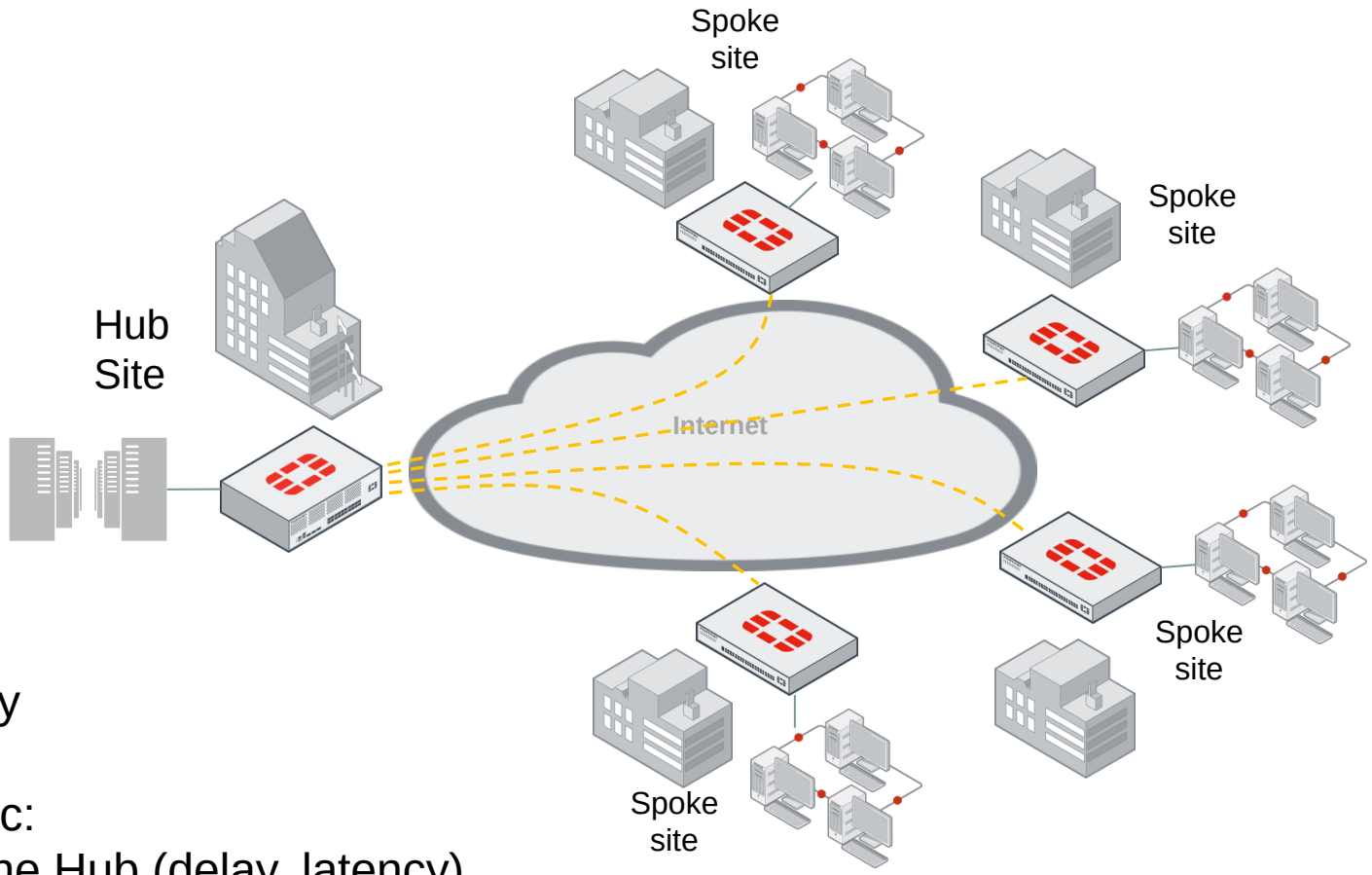
© Copyright Fortinet Inc. All rights reserved.

IPsec VPN Topology

How to organize the collection of point-to-point IPsec virtual links between all sites ?

Hub and Spoke

Hub nodes concentrate Spoke nodes in a Star topology



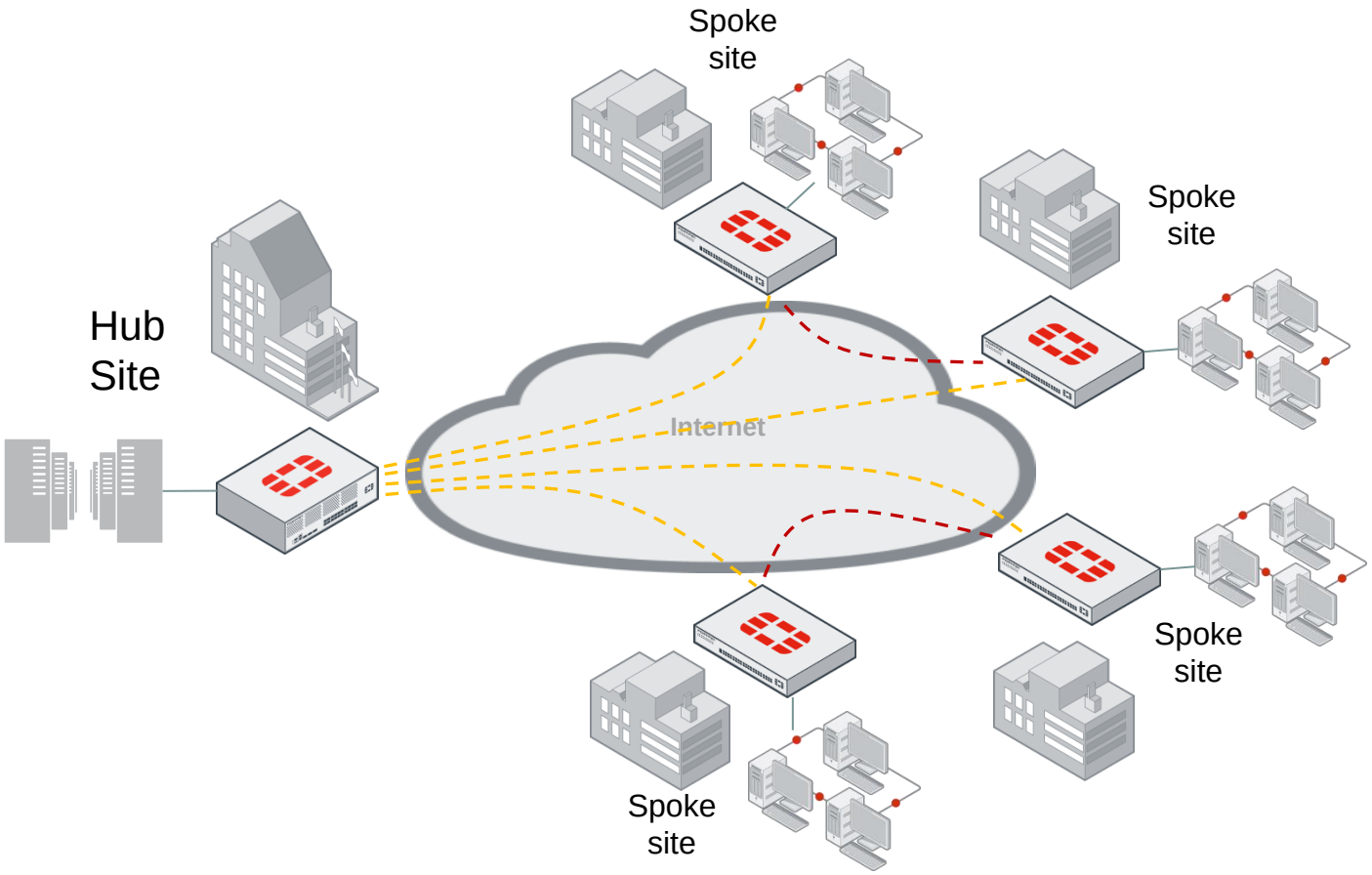
The simplest topology

Spoke to Spoke traffic:

- must go through the Hub (delay, latency)
- needlessly consume resources on Hub site (CPU, memory, Internet link)

Partial Mesh

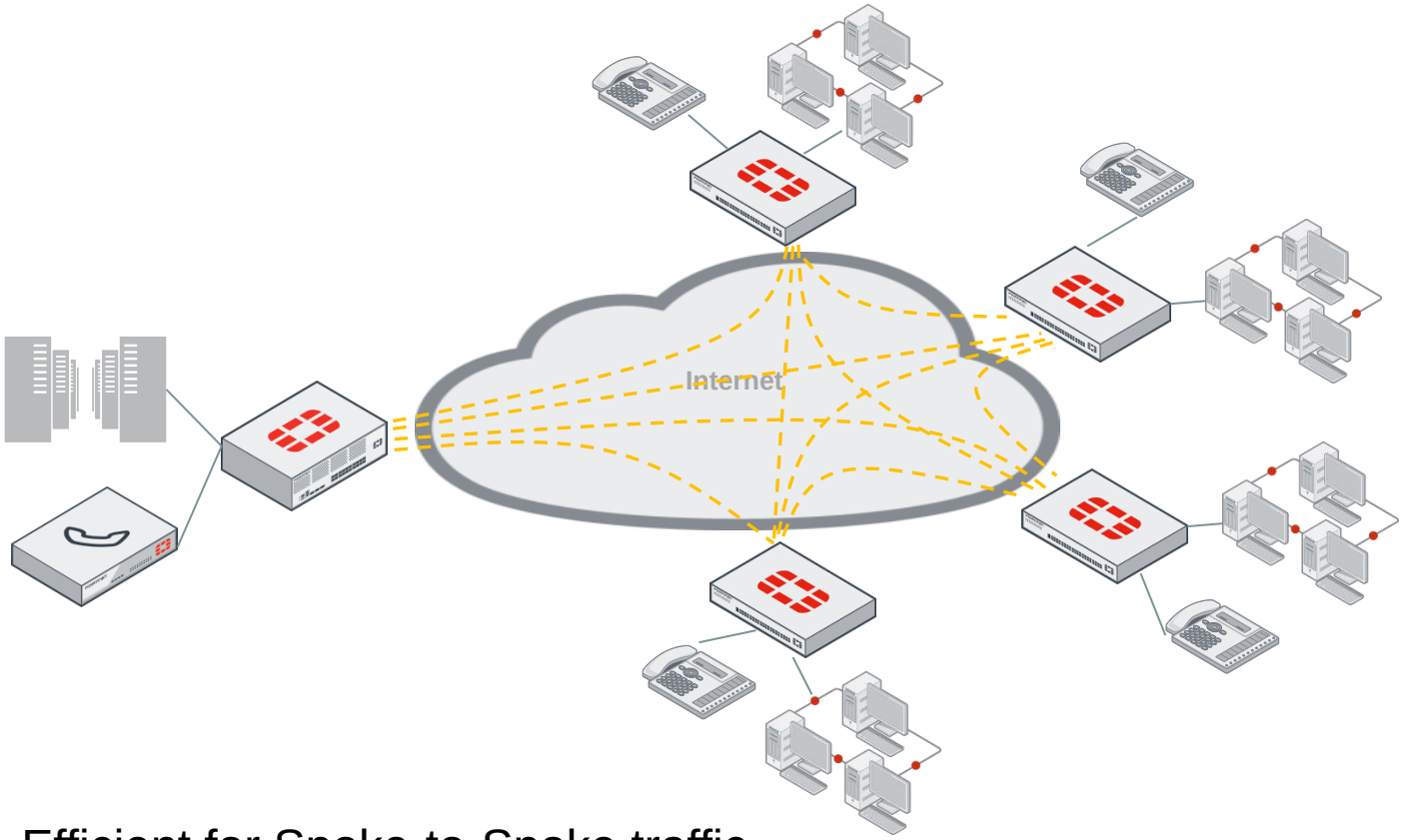
Typically a Hub-and-Spoke topology with additional direct tunnels between some Spokes



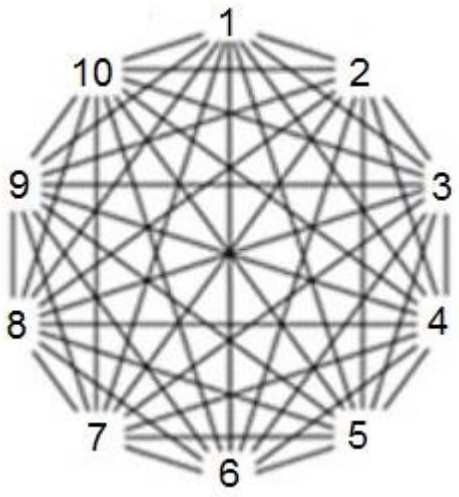
A middle ground between Hub-and-Spoke and Full-Mesh topologies

Full Mesh

Direct connectivity between all sites



N sites = N (N-1) / 2 tunnels

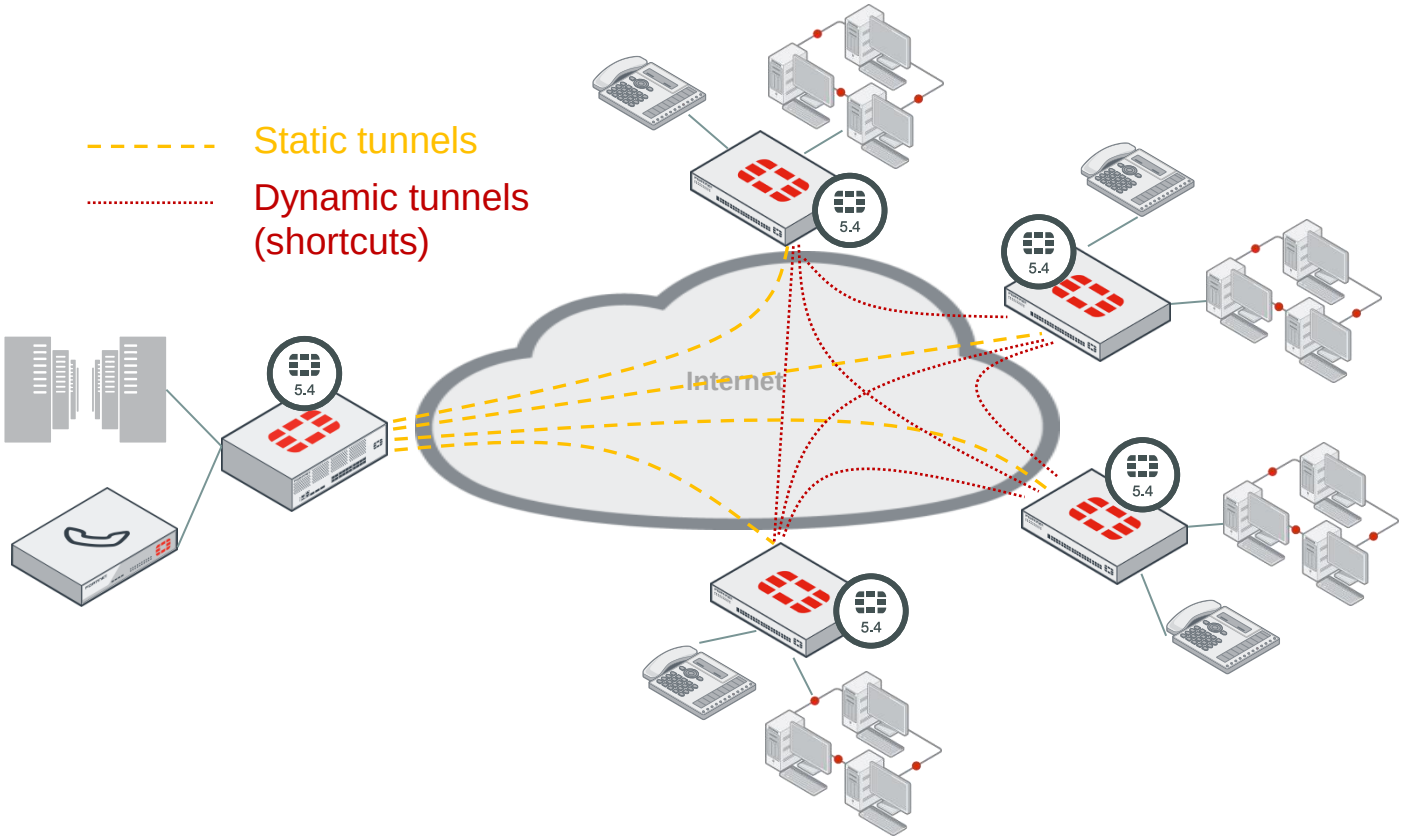


10 sites = 45 tunnels !

Efficient for Spoke-to-Spoke traffic
Complex configuration
Not scalable

Auto-Discovery VPN

Direct connectivity between all sites



« The simplicity of Hub & Spoke
with the
efficiency of Full-Mesh »

VPN configuration is as simple as configuring a simple Hub & Spoke setup

FortiOS ADVPN

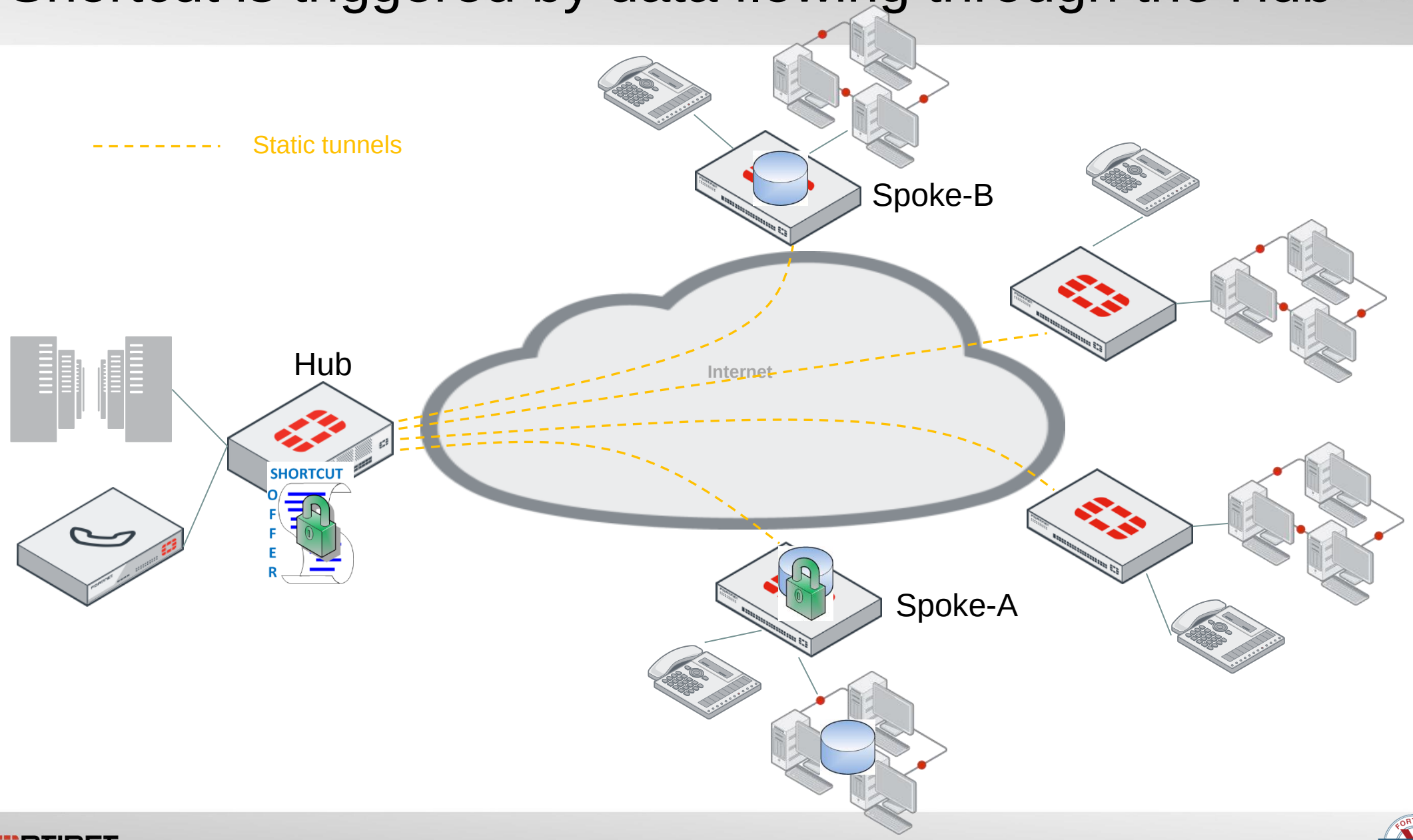
5.4

On-demand tunnels between Spokes

FORTINET

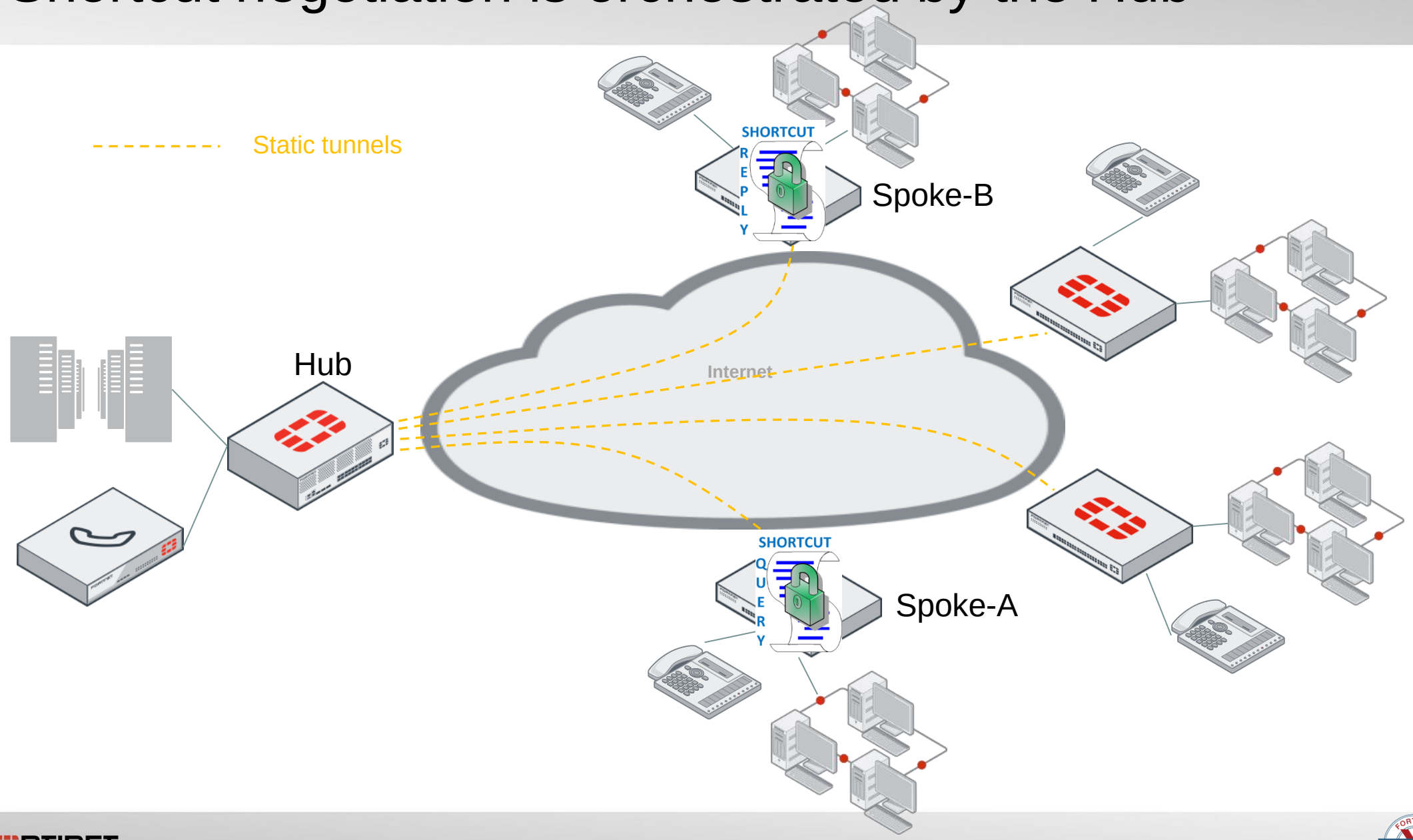
FORTINET XPERTS ACADEMY

1 Shortcut is triggered by data flowing through the Hub



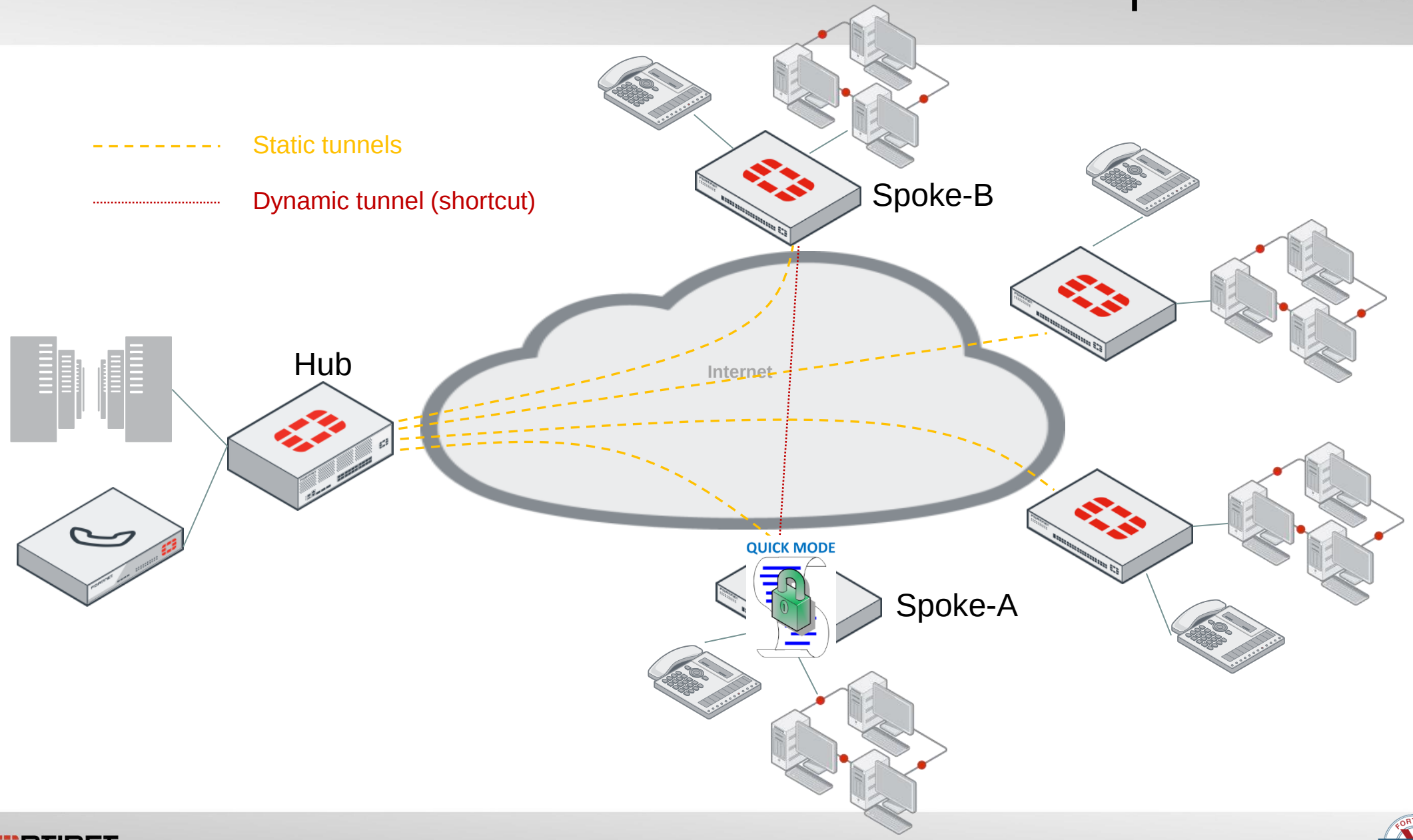
Animated Slide

2 Shortcut negotiation is orchestrated by the Hub



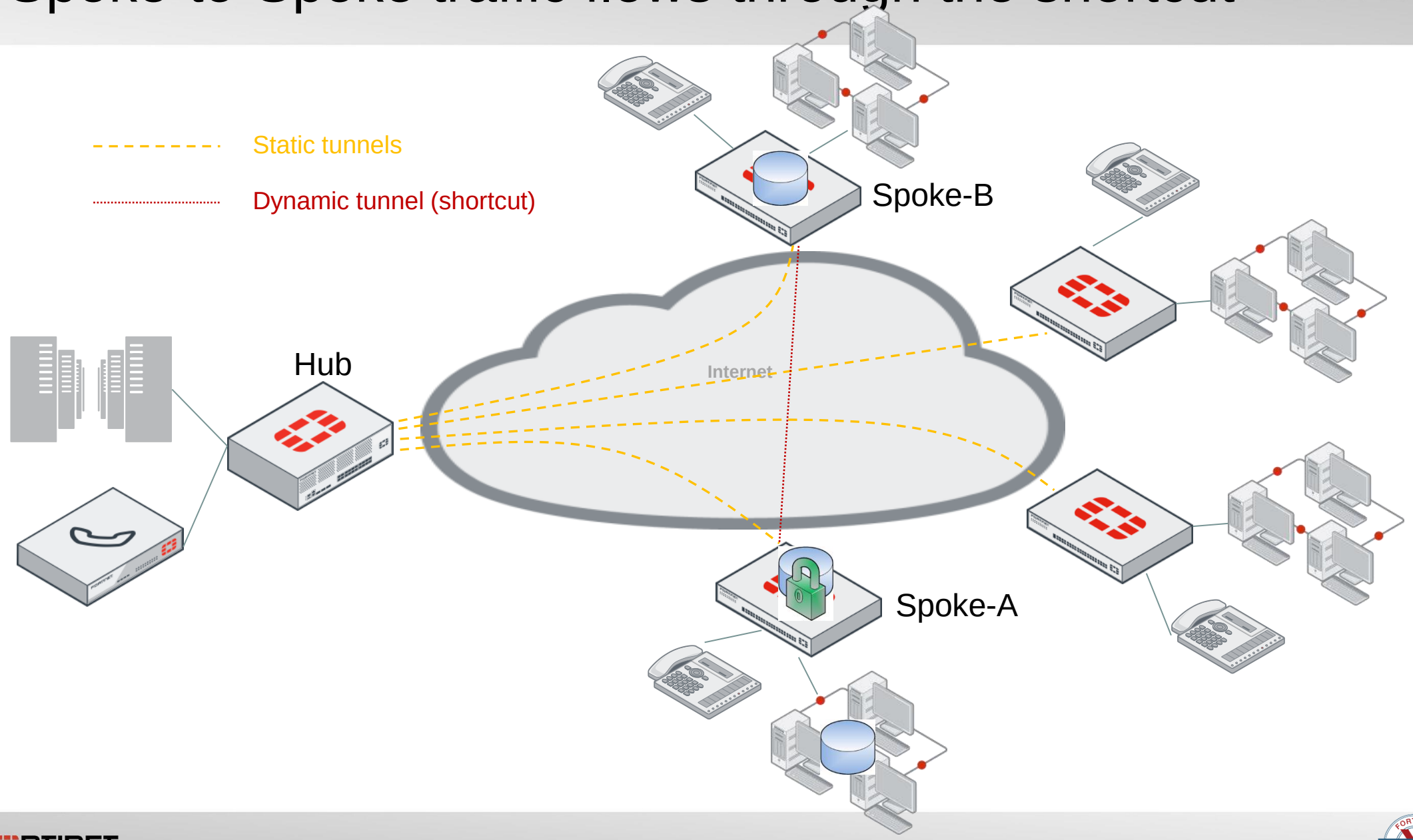
Animated Slide

3 Shortcut tunnel is established between the Spokes



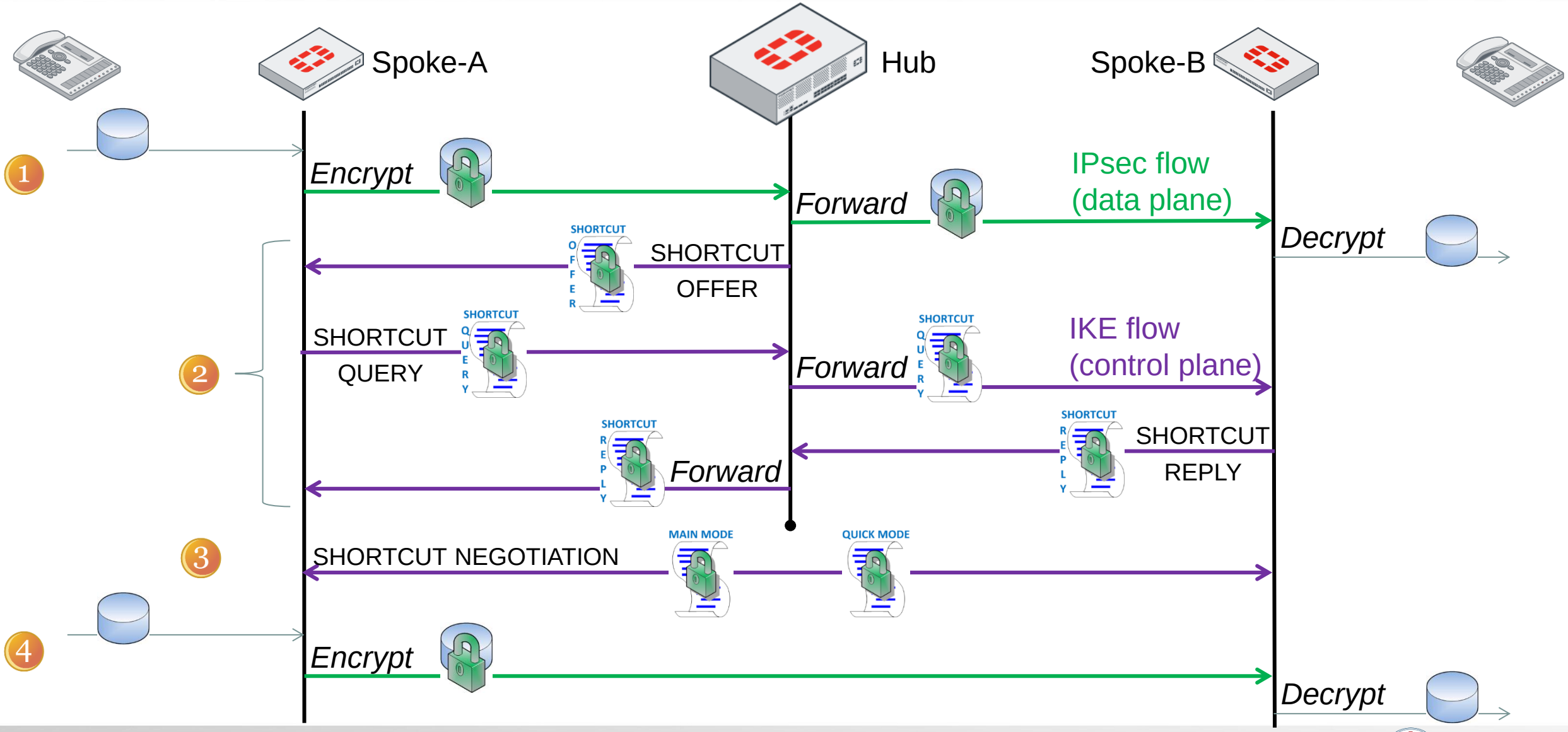
Animated Slide

4 Spoke-to-Spoke traffic flows through the shortcut



Animated Slide

Summary – ADVPN Sequence of Events



Fortinet Auto-Discovery VPN

Fortinet ADVPN is a proprietary solution solely based on IKE & IPsec

It is incompatible with Cisco DMVPN which relies on mGRE-over-IPsec and NHRP

IKE:

- Only IKEv1 main-mode is supported (pre-shared key and signature authentication)
- IKEv1 aggressive-mode and IKEv2 are not supported
- Both IPv4 & IPv6 are supported

Dynamic Routing:

- BGP and RIPv2/RIPng are supported
- OSPF, IS-IS and PIM are not supported

Fortinet Auto-Discovery VPN - FAQ

- Is it mandatory that the Hub runs FortiOS 5.4 ?

  Yes.
  The Hub is responsible for triggering the shortcut OFFER and for relaying the shortcut QUERY/REPLY between the Spokes. It must be running FortiOS 5.4 if shortcuts are desired.

- Is it mandatory that all Spokes be FortiGate running FOS 5.4 ?

  No.
  If a Spoke is not running FortiOS 5.4 or if it is an IPsec Gateway from another vendor, then it can still participate to the Hub & Spoke architecture but it will not be able to negotiate shortcuts with other Spokes.
  Mixing ADVPN-aware and non-ADVPN IPsec gateways on the same phase1 requires specific configuration on the Hub and the non-ADVPN gateways.

Fortinet Auto-Discovery VPN - FAQ

- Can some of my Spokes be NATed ?

  Yes.
  A shortcut can be established between two Spokes as long as one of the two is not NATed.
  A shortcut cannot be established between two Spokes that are both NATed.

- Can shortcuts be torn down when they are idle ?

  Yes.
  It can be configured per Spoke under the phase1 connected the Hub:

```
config vpn ipsec phase1-interface
edit <to-the-Hub>
        set idle-timeout enable                    // default= disable
        set idle-timeoutinterval <in_minutes>      // default=15, range=[10 ; 43200]
end
```

Fortinet Auto-Discovery VPN - FAQ

- I would like to spread the Spokes between my two ISPs (wan1, wan2).
  Will the Spokes bound to the phase1 on wan1 be able to establish shortcuts with the Spokes bound to the phase1 on wan2 ?

  Yes.
  No additional configuration is required to cover this scenario.

- I have two independent Hub & Spoke architectures (Hub-A H&S and Hub-B H&S). Is it possible to establish shortcuts between the Spokes of Hub-A and the Spokes of Hub-B ?

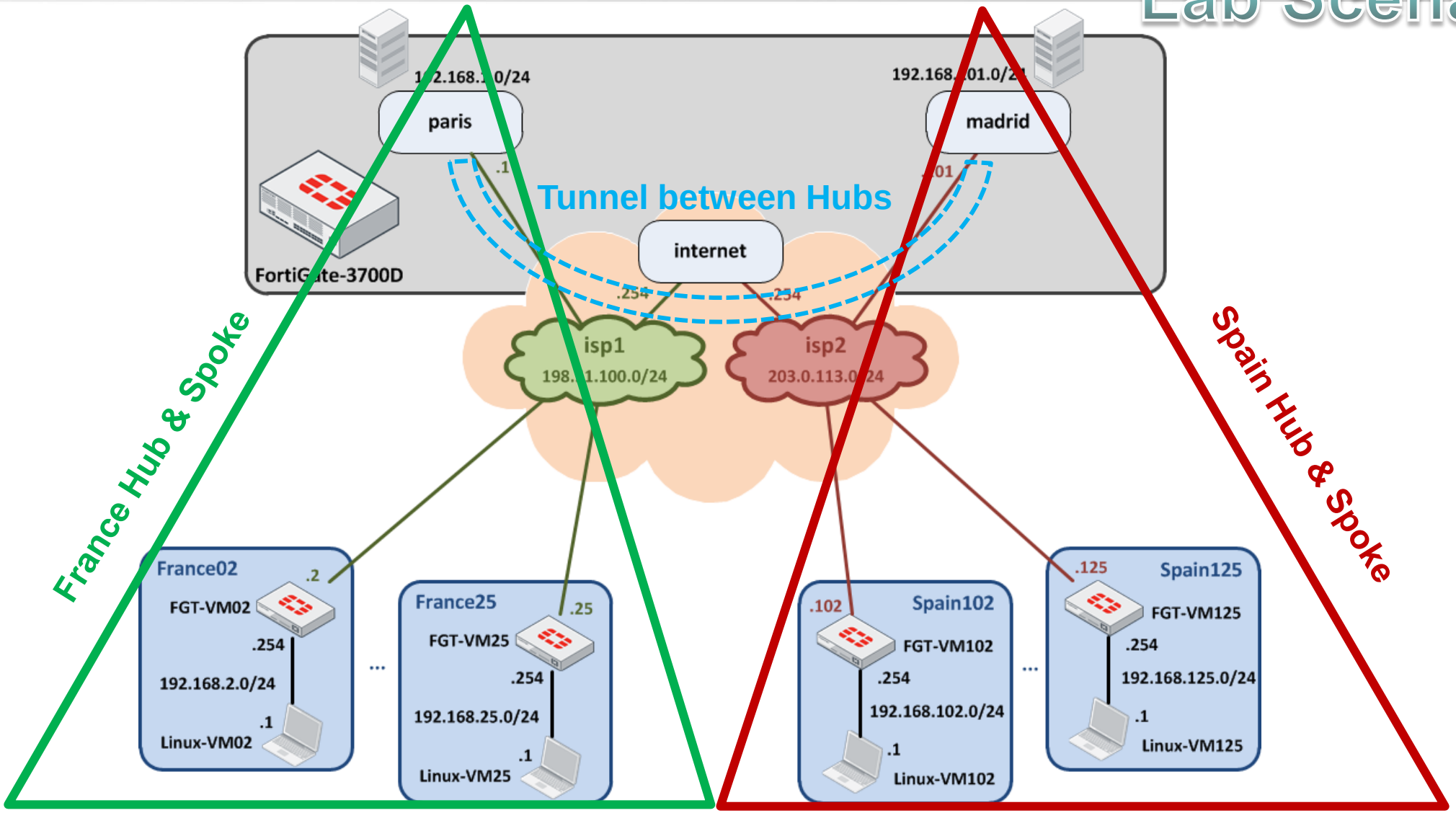
  Yes.
  It requires that an IPsec tunnel be configured between Hub-A and Hub-B and that a specific ADVPN setting be enabled on this tunnel (`auto-discovery-forwarder`).

ADVPN configuration

IPsec configuration

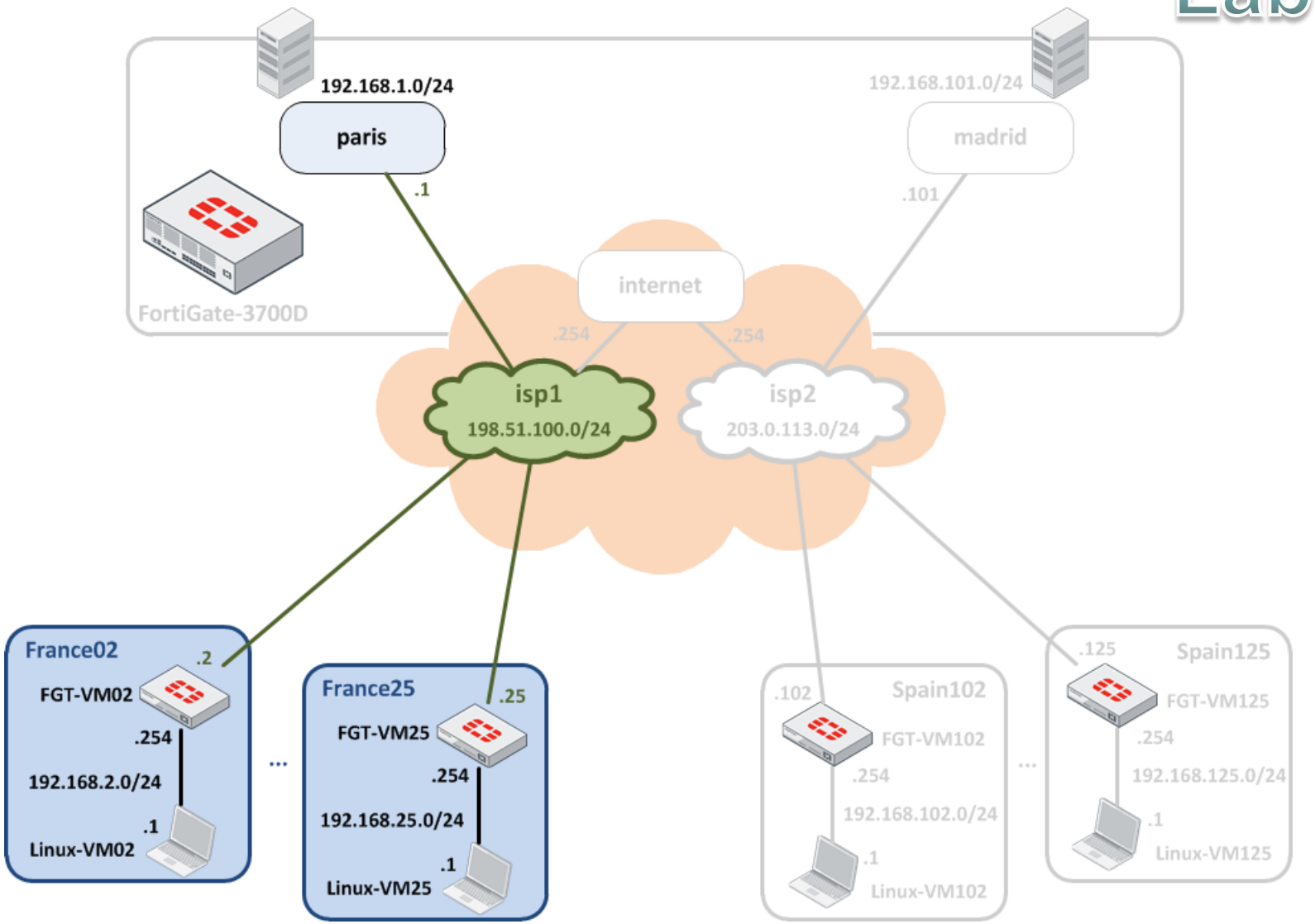
Hub & Spoke Architecture

Xpert Academy
Lab Scenario



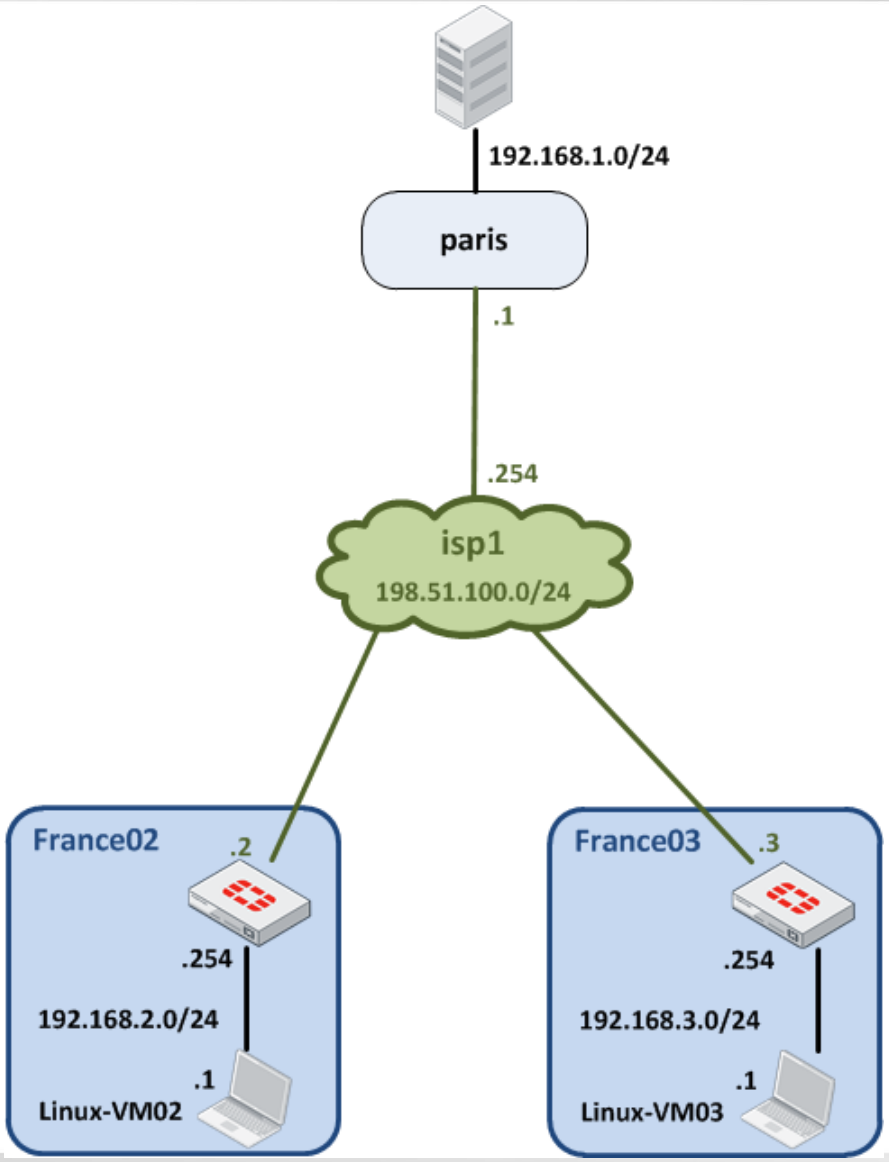
France Hub & Spoke Network

Xpert Academy
Lab Scenario



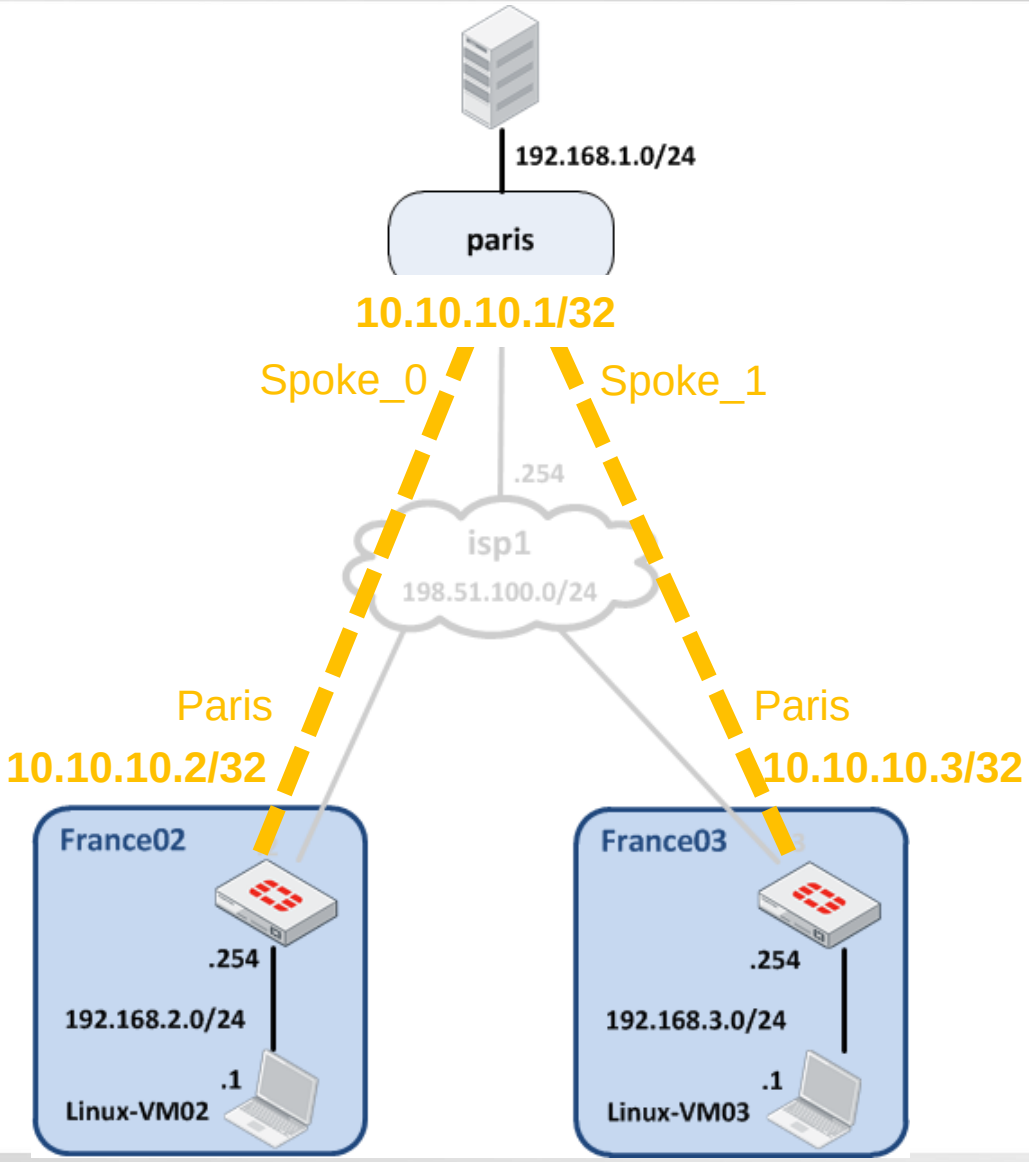
France Hub & Spoke Network

Xpert Academy
Lab Scenario



France Hub & Spoke Overlay subnet

Xpert Academy
Lab Scenario



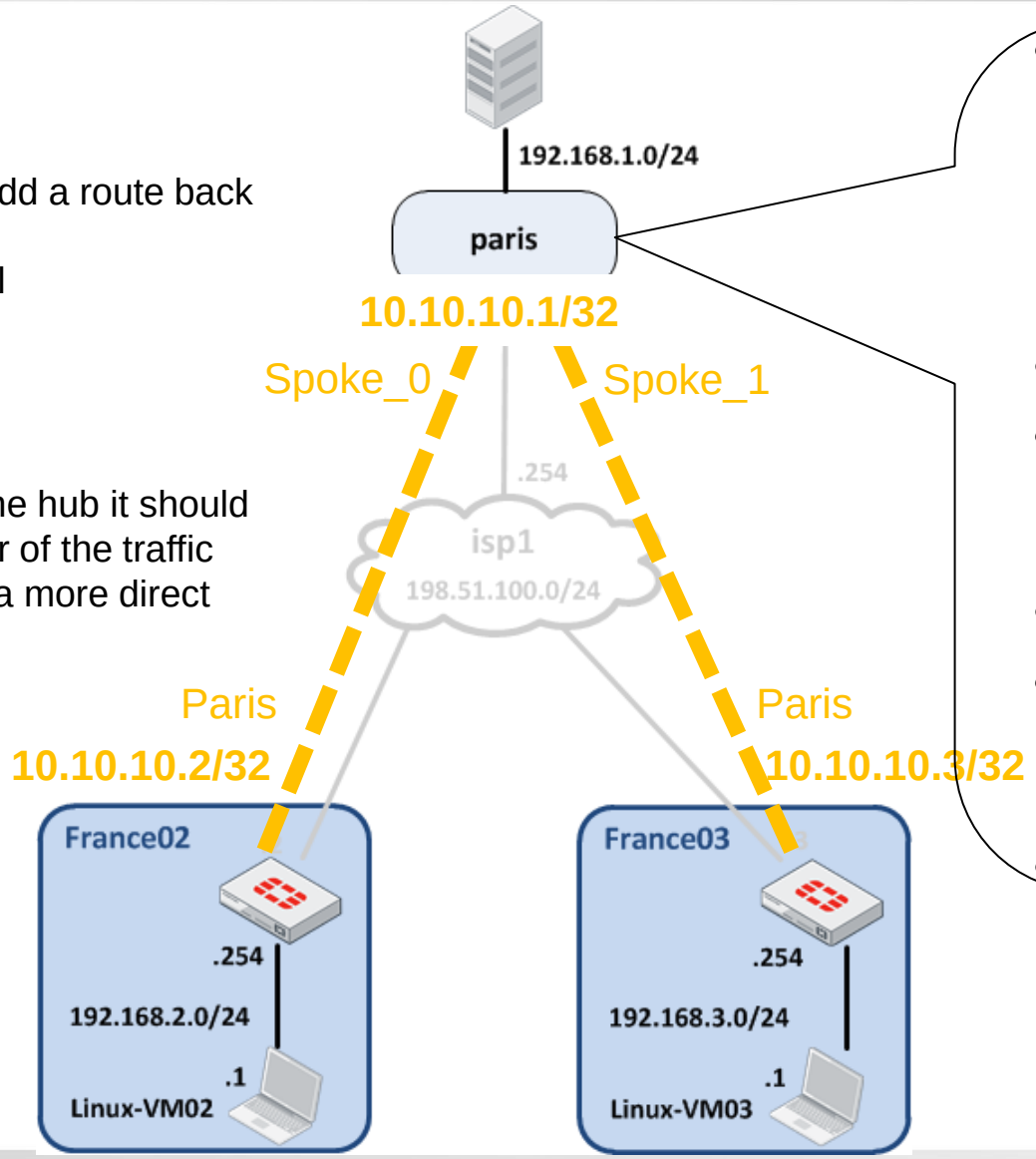
ADVPN Hub configuration

add-route disable

ensures that IKE does not automatically add a route back over the spoke and instead leaves routing to a separately configured routing protocol

auto-discovery-sender enable

Indicates that when IPsec traffic transits the hub it should send a SHORTCUT-OFFER to the initiator of the traffic to indicate that it could perhaps establish a more direct connection (shortcut)

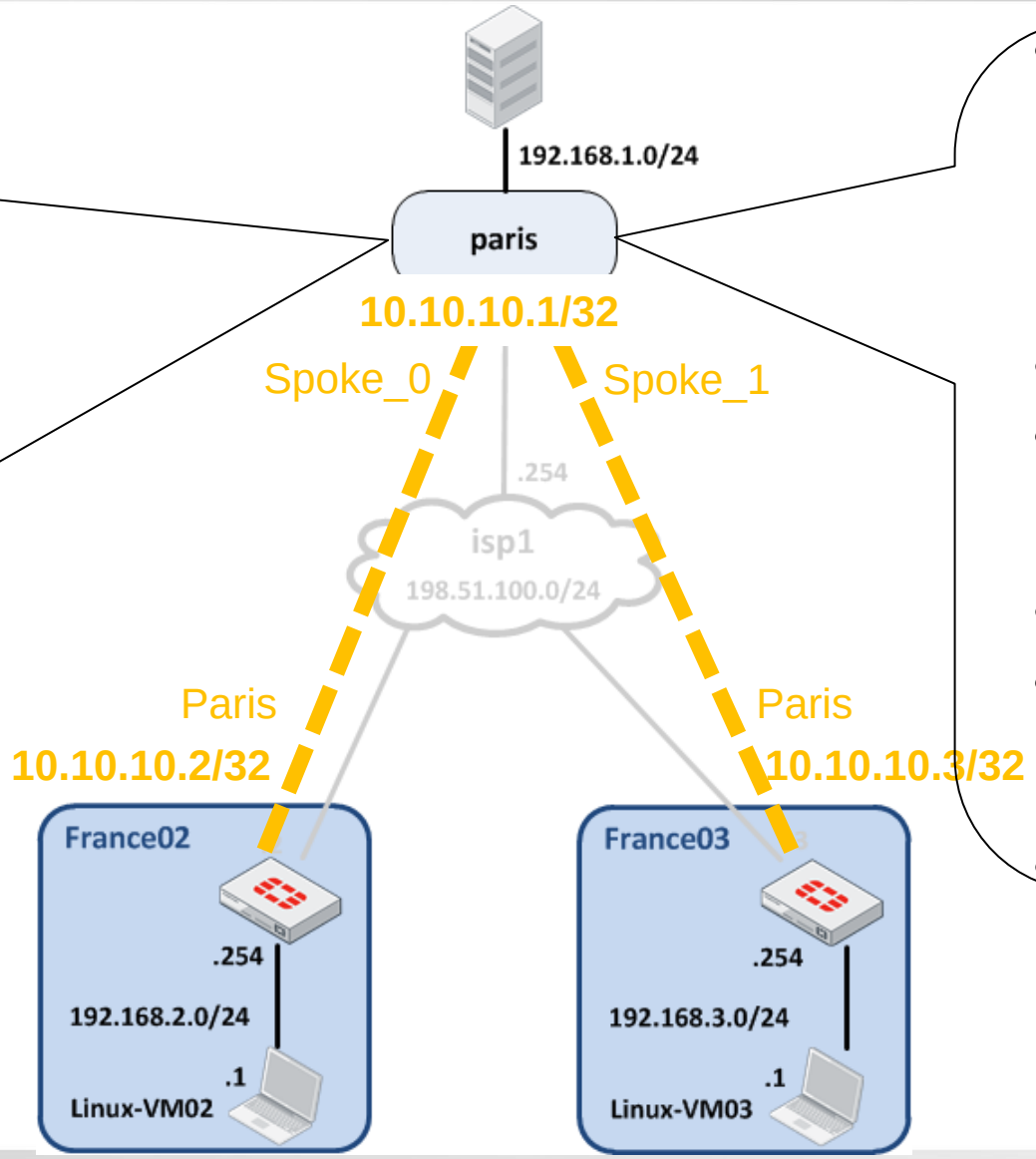



```
config vpn ipsec phase1-interface
    edit "Spoke"
        set type dynamic
        set interface "wan1"
        set proposal aes128-sha1
        set add-route disable
        set auto-discovery-sender enable
        set psksecret fortinet
    next
end

config vpn ipsec phase2-interface
    edit "Spoke"
        set phase1name "Spoke"
        set proposal aes128-sha1
    next
end

config system interface
    edit "Spoke"
        set ip 10.10.10.1/32
        set remote-ip 10.10.10.254
    next
end
```

The `remote-ip` is dummy
It can be any unused IP

ADVPN Hub configuration

```
config firewall policy
    edit 1
        set name "To Spokes"
        set srcintf "internal"
        set dstintf "Spoke"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "From Spokes"
        set srcintf "Spoke"
        set dstintf "internal"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 3
        set name "Spokes to Spokes"
        set srcintf "Spoke"
        set dstintf "Spoke"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

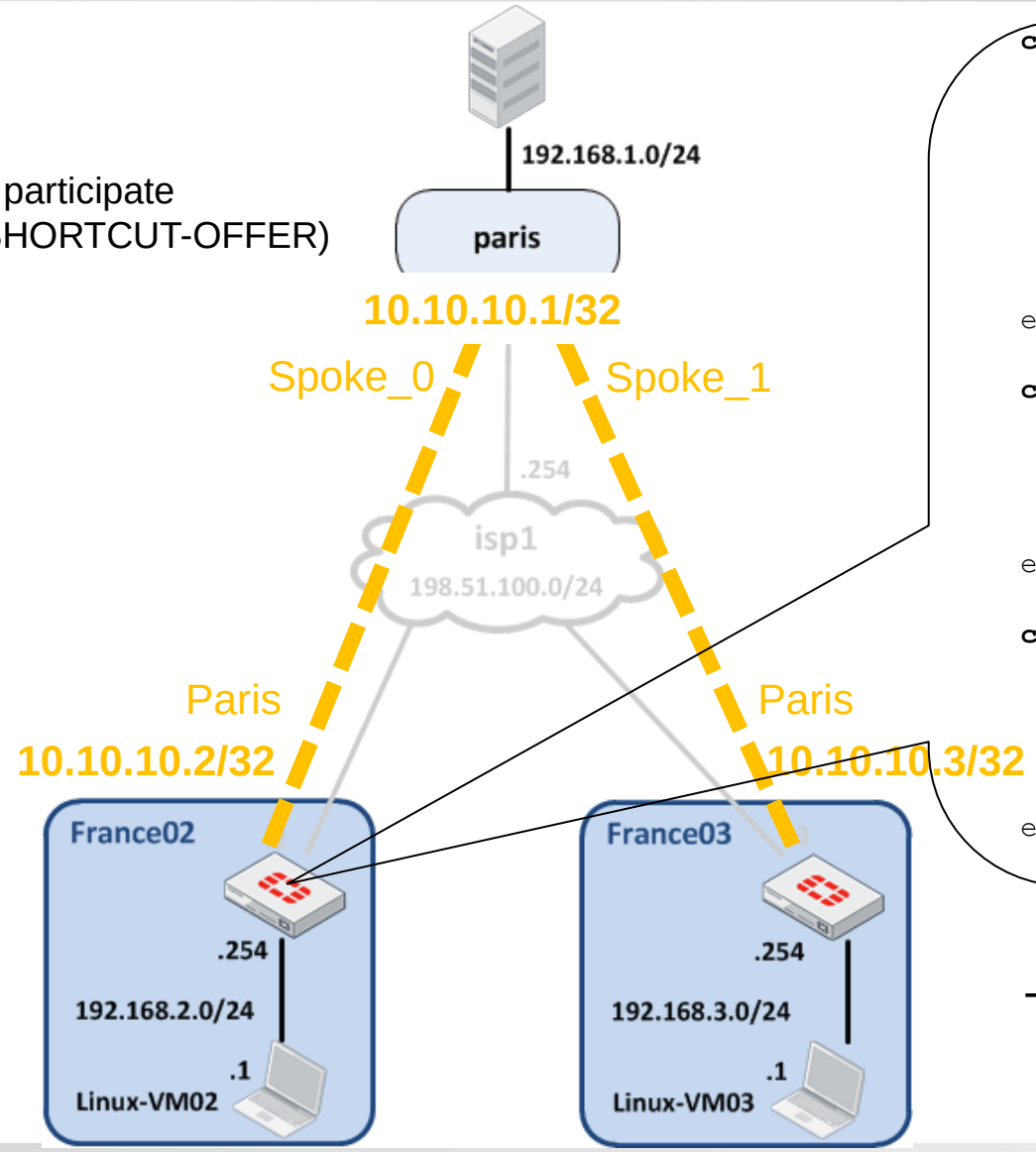



```
config vpn ipsec phase1-interface
    edit "Spoke"
        set type dynamic
        set interface "wan1"
        set proposal aes128-sha1
        set add-route disable
        set auto-discovery-sender enable
        set psksecret fortinet
    next
end

config vpn ipsec phase2-interface
    edit "Spoke"
        set phase1name "Spoke"
        set proposal aes128-sha1
    next
end

config system interface
    edit "Spoke"
        set ip 10.10.10.1/32
        set remote-ip 10.10.10.254
    next
end
```

ADVPN Spoke configuration

auto-discovery-receiver enable

To indicate that this IPsec tunnel wishes to participate in an Auto-Discovery VPN (i.e., receive a SHORTCUT-OFFER)

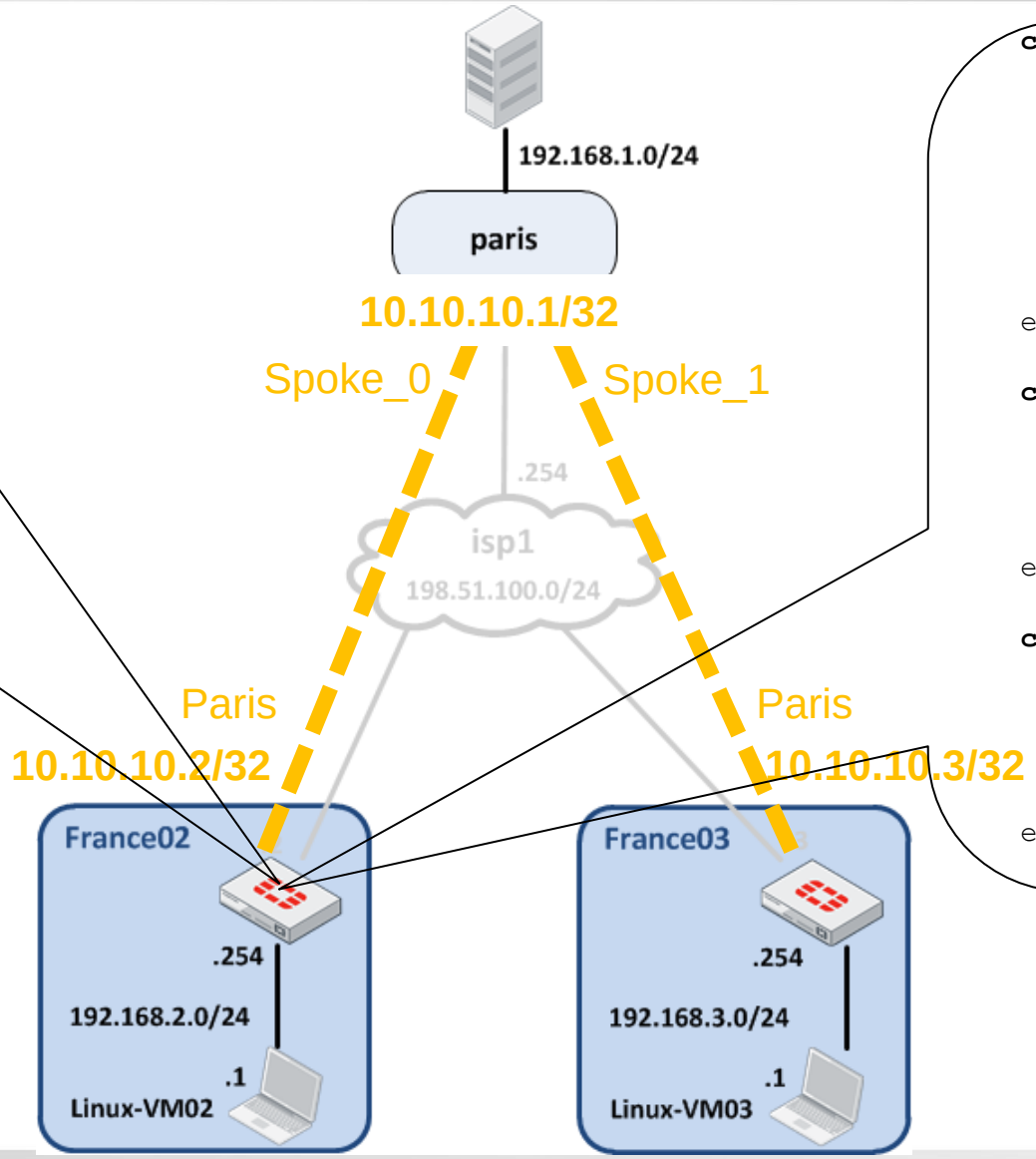



```
config vpn ipsec phase1-interface
    edit "Paris"
        set interface "wan1"
        set proposal aes128-sha1
        set auto-discovery-receiver enable
        set remote-gw 198.51.100.1
        set psksecret fortinet
    next
end

config vpn ipsec phase2-interface
    edit "Paris"
        set phase1name "Paris"
        set proposal aes128-sha1
    next
end

config system interface
    edit "Paris"
        set ip 10.10.10.2/32
        set remote-ip 10.10.10.1
    next
end
```

The `remote-ip` is the IP of the Hub

ADVPN Spoke configuration

```
config firewall policy
    edit 1
        set name "To Hub/Spokes"
        set srcintf "internal"
        set dstintf "Paris"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "From Hub/Spokes"
        set srcintf "Paris"
        set dstintf "internal"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```




```
config vpn ipsec phase1-interface
    edit "Paris"
        set interface "wan1"
        set proposal aes128-sha1
        set auto-discovery-receiver enable
        set remote-gw 198.51.100.1
        set psksecret fortinet
    next
end

config vpn ipsec phase2-interface
    edit "Paris"
        set phase1name "Paris"
        set proposal aes128-sha1
    next
end

config system interface
    edit "Paris"
        set ip 10.10.10.2/32
        set remote-ip 10.10.10.1
    next
end
```

No specific policies are needed for traffic to/from other Spokes.

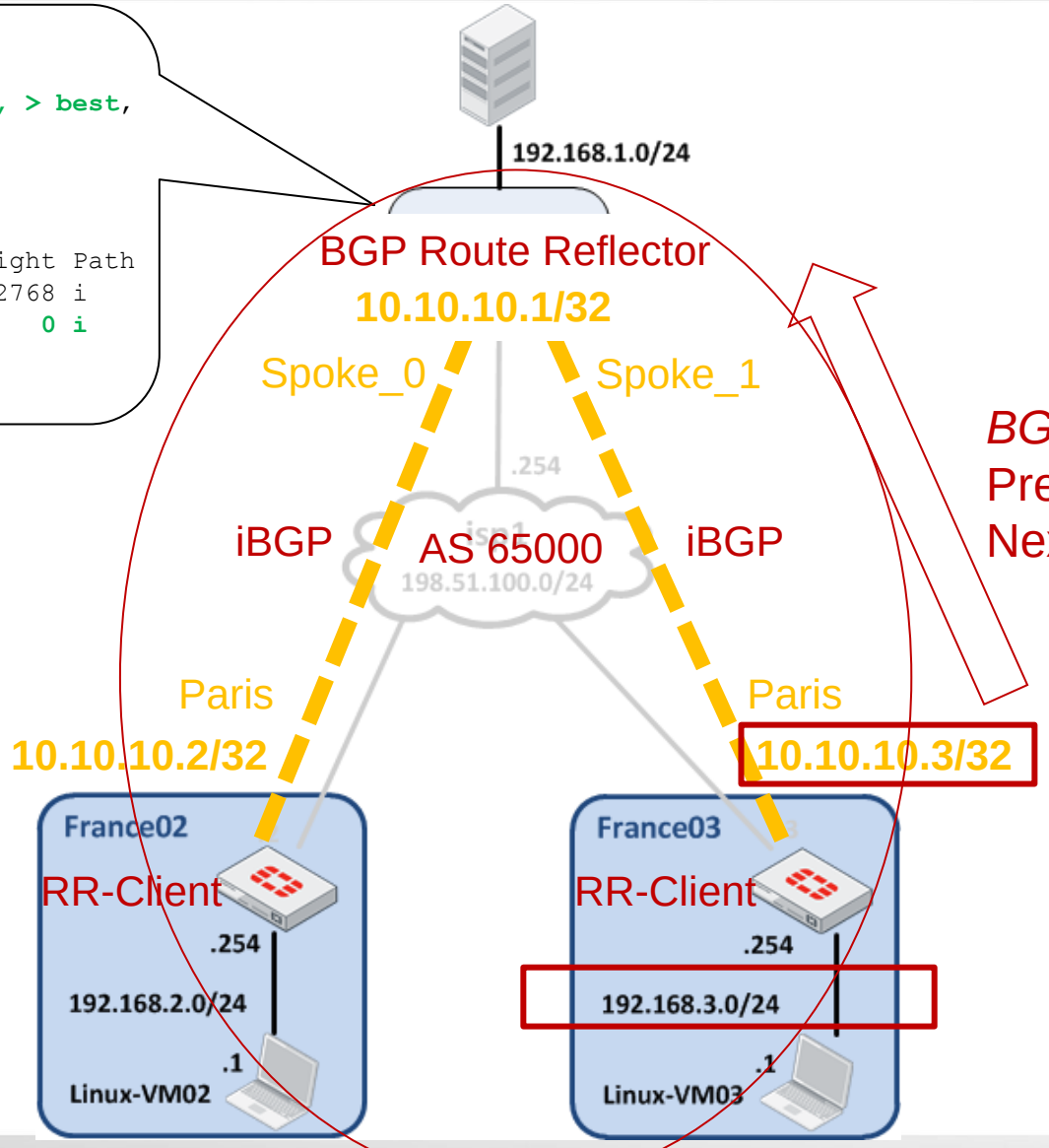
Traffic to/from other Spokes is checked against the policies to/from the Hub

ADVPN with BGP dynamic routing

iBGP with Route-Reflector

iBGP – Route Reflector (RR) and RR-Clients

```
Paris # get router info bgp network
BGP table version is 4, local router ID is 10.10.10.1
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      0.0.0.0                     100  32768 i
*>i192.168.3.0      10.10.10.3               0    100      0 i

Total number of prefixes 2
```



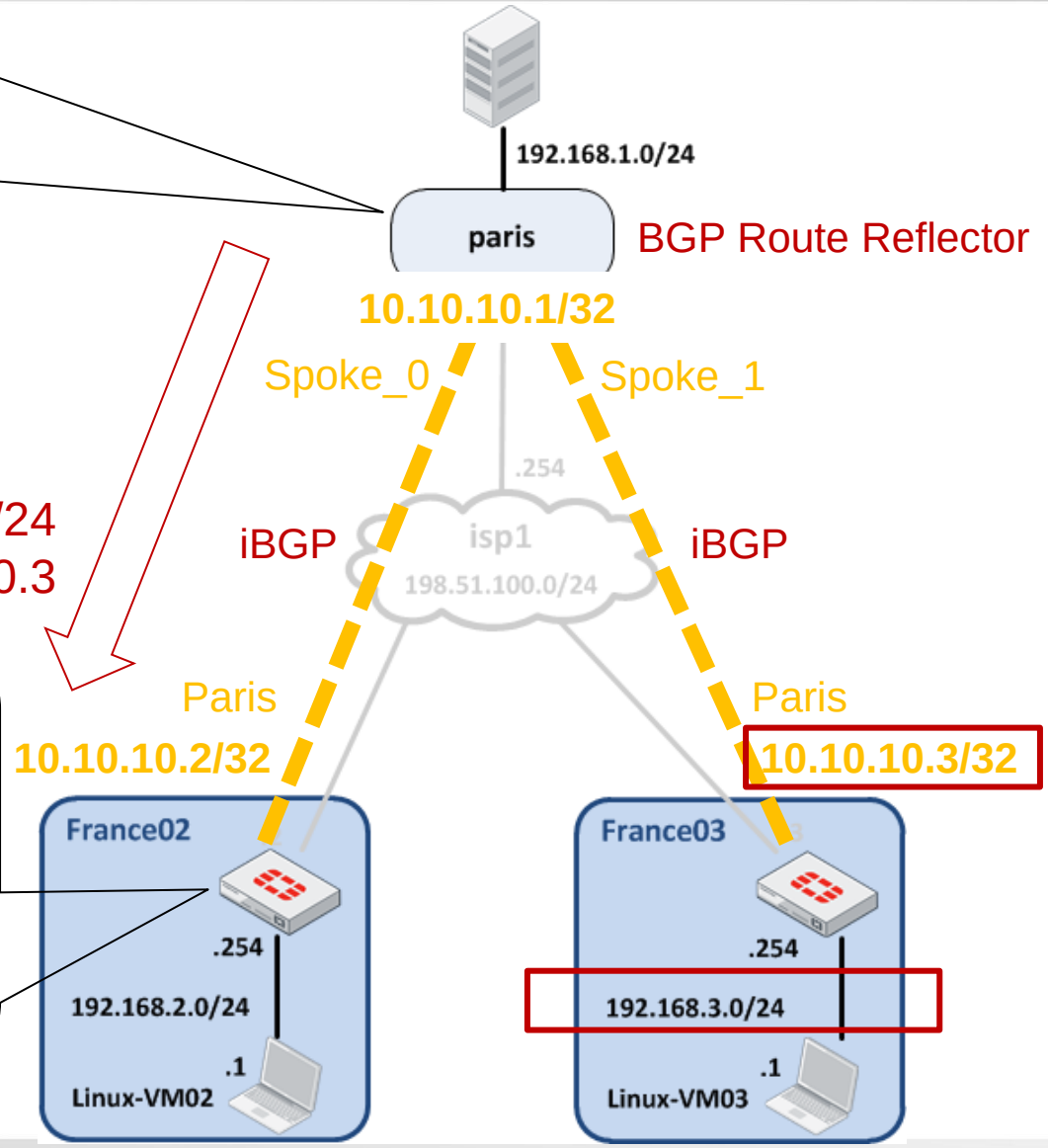
BGP Update:
Prefix= 192.168.3.0/24
Next-Hop = 10.10.10.3

iBGP – Route Reflector (RR) and RR-Clients

```
Paris # get router info bgp network
BGP table version is 4, local router ID is 10.10.10.1
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      0.0.0.0                     100  32768 i
*>i192.168.3.0      10.10.10.3               0    100      0 i

Total number of prefixes 2
```

BGP Update:
Prefix= 192.168.3.0/24
Next-Hop = 10.10.10.3

```
France02 # get router info bgp network
BGP table version is 4, local router ID is 10.10.10.2
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i192.168.1.0      10.10.10.1               0    100      0 i
*> 192.168.2.0      0.0.0.0                     100  32768 i
*>i192.168.3.0      10.10.10.3               0    100      0 i

Total number of prefixes 3
```



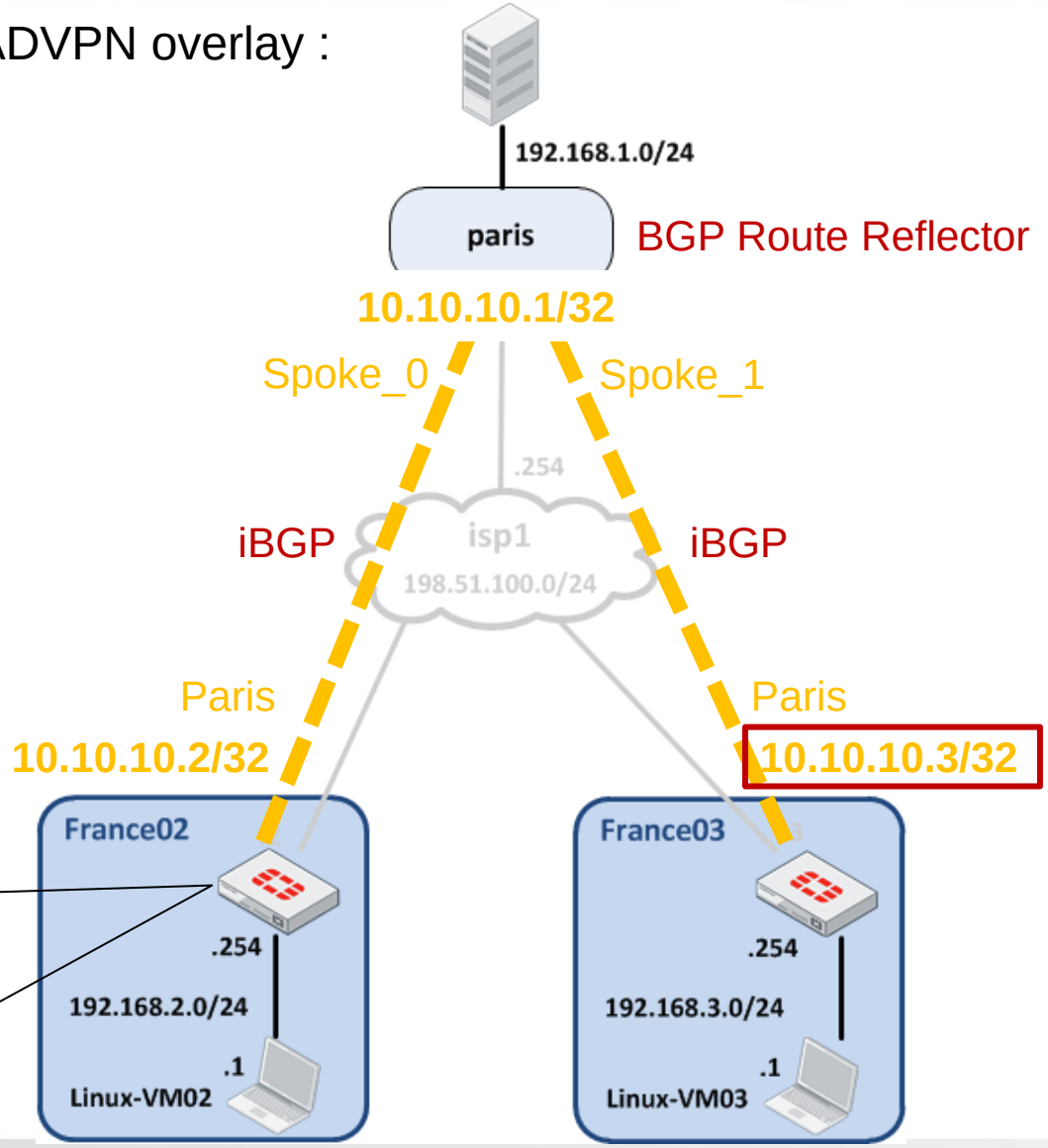
iBGP Next Hop Reachability

On each Spoke, add a static route covering the ADVPN overlay :

```
config router static
    edit 0
        set dst 10.10.10.0 255.255.255.0
        set device "Paris"
        set comment "ADVPN overlay subnet"
    next
end
```

BGP Next-Hop must be accessible through the tunnel

```
France02 # get router info bgp network
BGP table version is 4, local router ID is 10.10.10.2
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i192.168.1.0      10.10.10.1               0    100      0 i
*> 192.168.2.0      0.0.0.0                       100  32768 i
*>i192.168.3.0      10.10.10.3               0    100      0 i

Total number of prefixes 2
```



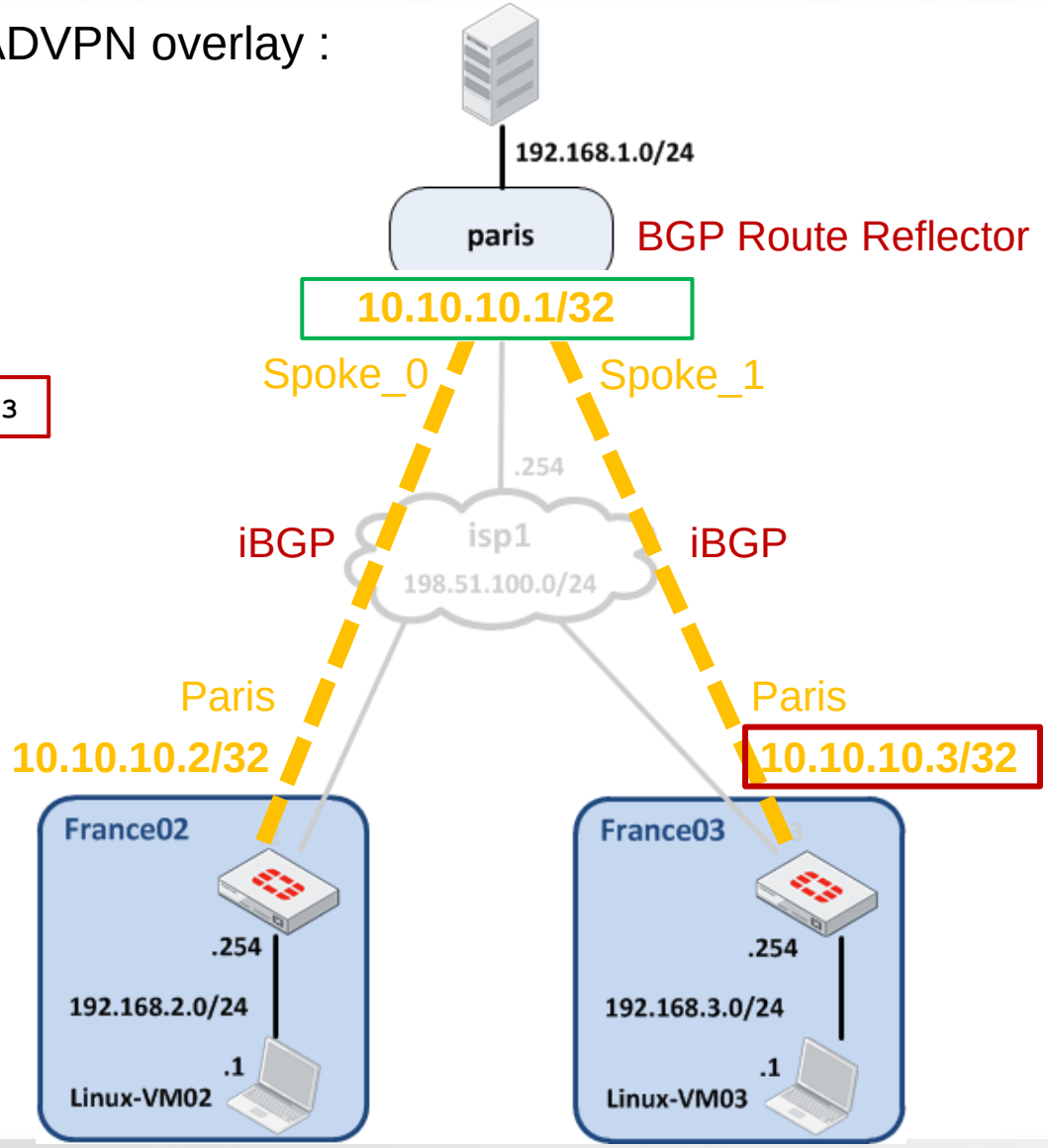
No shortcut – BGP Next-Hop is reached via the Hub

On each Spoke, add a static route covering the ADVPN overlay :

```
config router static
    edit 0
        set dst 10.10.10.0 255.255.255.0
        set device "Paris"
        set comment "ADVPN overlay subnet"
    next
end
```

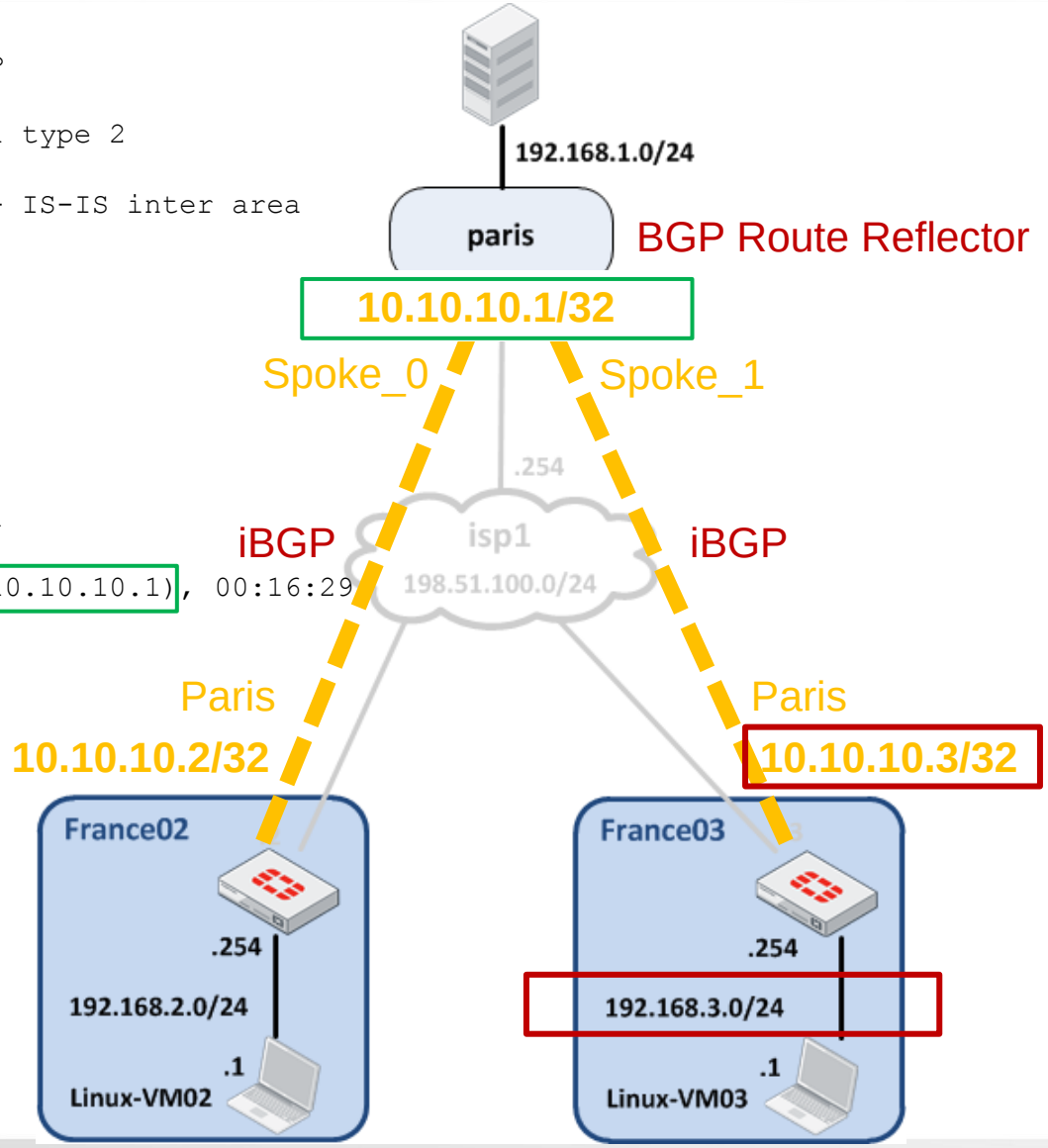
```
France02 # get router info routing-table details 10.10.10.3
Routing entry for 10.10.10.0/24
  Known via "static", distance 10, metric 0, best
  * 10.10.10.1, via Paris
```

BGP Next-Hop of France03 Spoke (10.10.10.3) is accessible via Paris Hub (10.10.10.1)



No shortcut – Recursive RIB lookup

```
France02 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 198.51.100.254, wan1

S       10.10.10.0/24 [10/0] via 10.10.10.1, Paris
C       10.10.10.1/32 is directly connected, Paris
C       10.10.10.2/32 is directly connected, Paris

B       192.168.1.0/24 [200/0] via 10.10.10.1, Paris, 02:01:11
C       192.168.2.0/24 is directly connected, internal
B       192.168.3.0/24 [200/0] via 10.10.10.3 (recursive via 10.10.10.1), 00:16:29

C       198.51.100.0/24 is directly connected, wan1
```

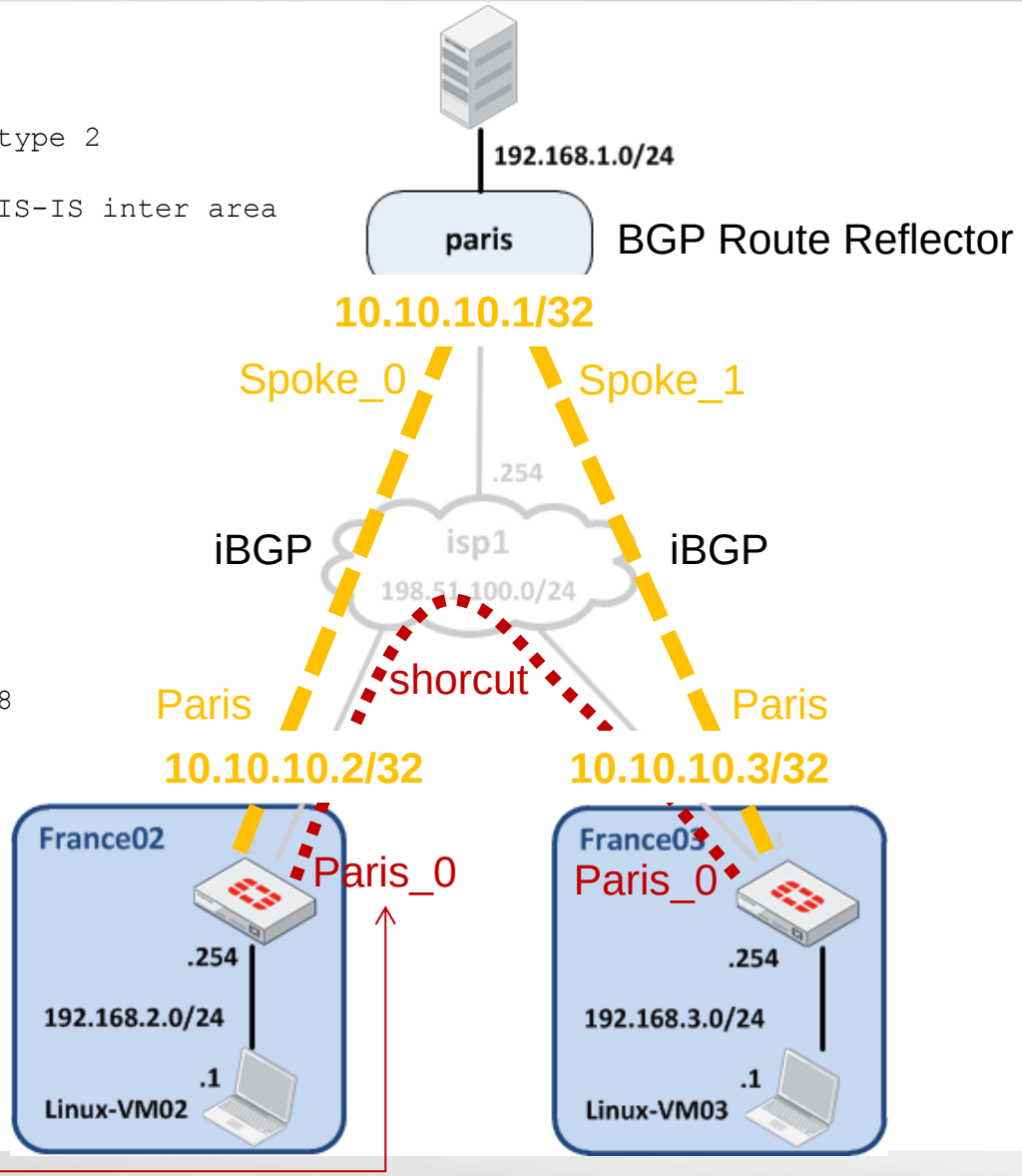


Spoke-to-Spoke traffic flows through the Hub

ADVPN Overlay with shortcut

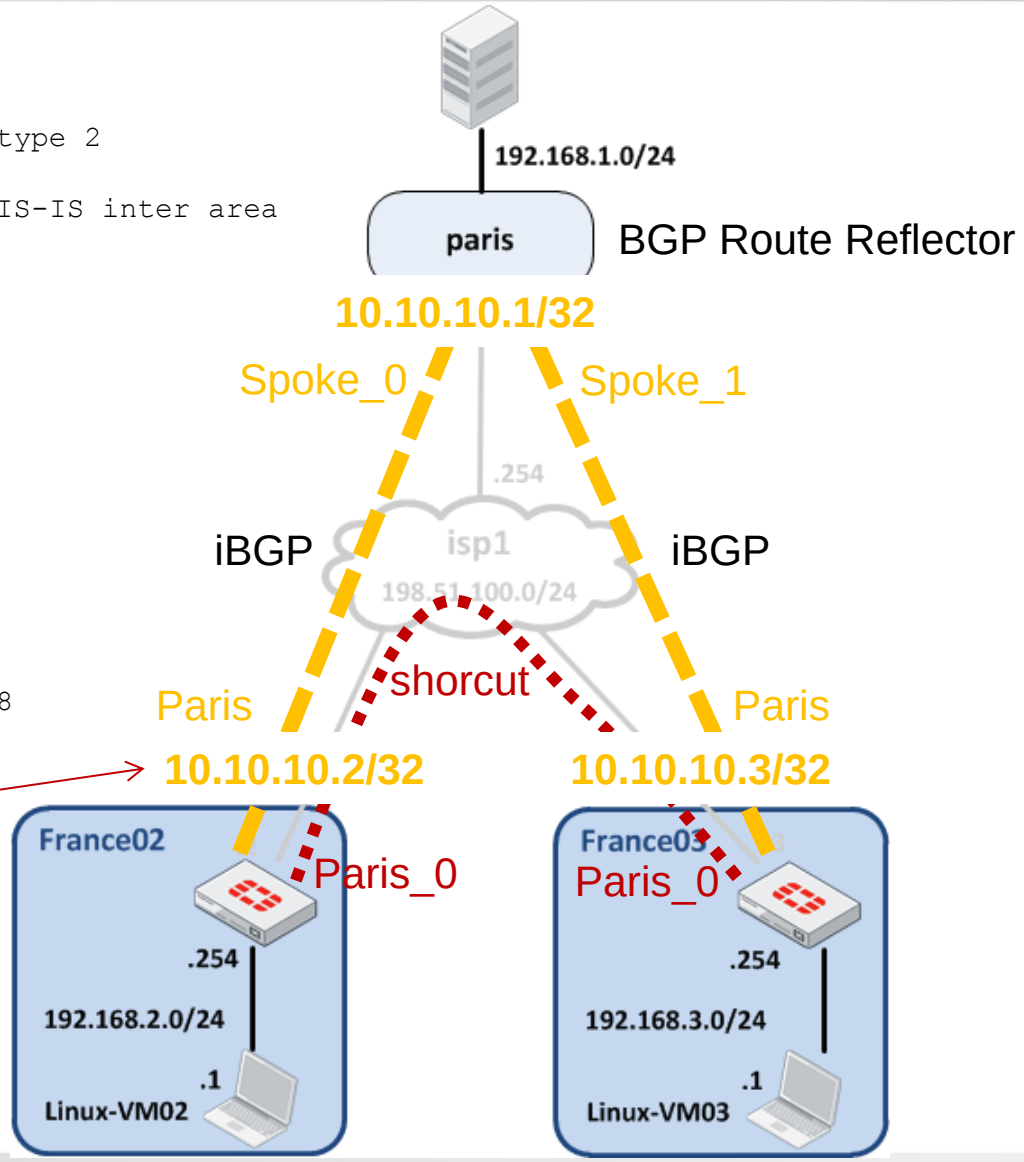
```
France02 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 198.51.100.254, wan1

S       10.10.10.0/24 [10/0] via 10.10.10.1, Paris

C       10.10.10.1/32 is directly connected, Paris
C       10.10.10.2/32 is directly connected, Paris
                      is directly connected, Paris_0
C       10.10.10.3/32 is directly connected, Paris_0

B       192.168.1.0/24 [200/0] via 10.10.10.1, Paris, 02:38:15
C       192.168.2.0/24 is directly connected, internal
B       192.168.3.0/24 [200/0] via 10.10.10.3, Paris_0, 00:00:28

C       198.51.100.0/24 is directly connected, wan1
```

Shortcut name = <phase1name>_<index>



ADVPN Overlay with shortcut

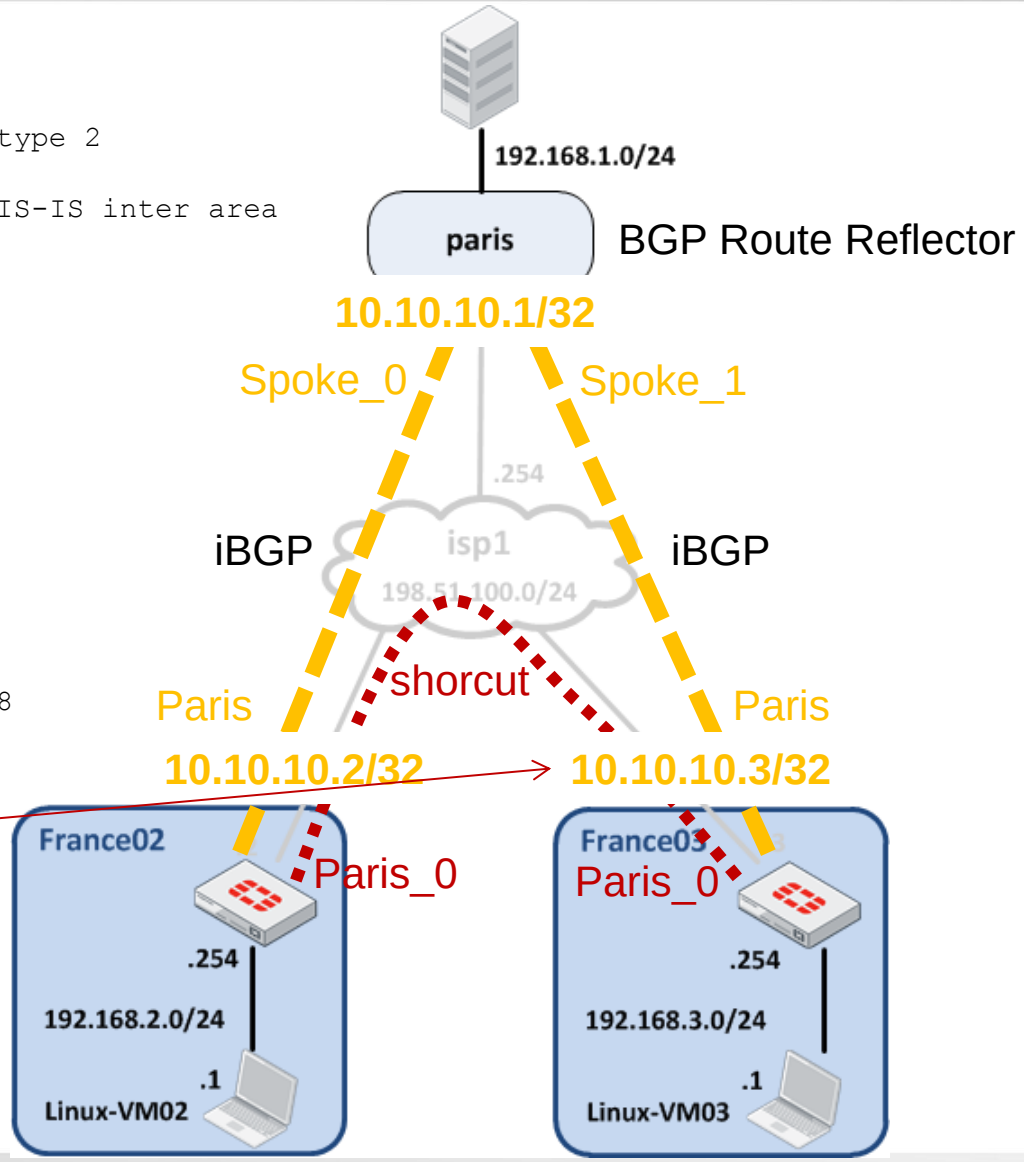
```
France02 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 198.51.100.254, wan1

S       10.10.10.0/24 [10/0] via 10.10.10.1, Paris

C       10.10.10.1/32 is directly connected, Paris
C       10.10.10.2/32 is directly connected, Paris
                      is directly connected, Paris_0
C       10.10.10.3/32 is directly connected, Paris_0

B       192.168.1.0/24 [200/0] via 10.10.10.1, Paris, 02:38:15
C       192.168.2.0/24 is directly connected, internal
B       192.168.3.0/24 [200/0] via 10.10.10.3, Paris_0, 00:00:28

C       198.51.100.0/24 is directly connected, wan1
```



The same overlay IP is assigned to:
- the tunnel toward the Hub
- the shortcut(s) toward other Spoke(s)

With shortcut – BGP Next-Hop is directly connected

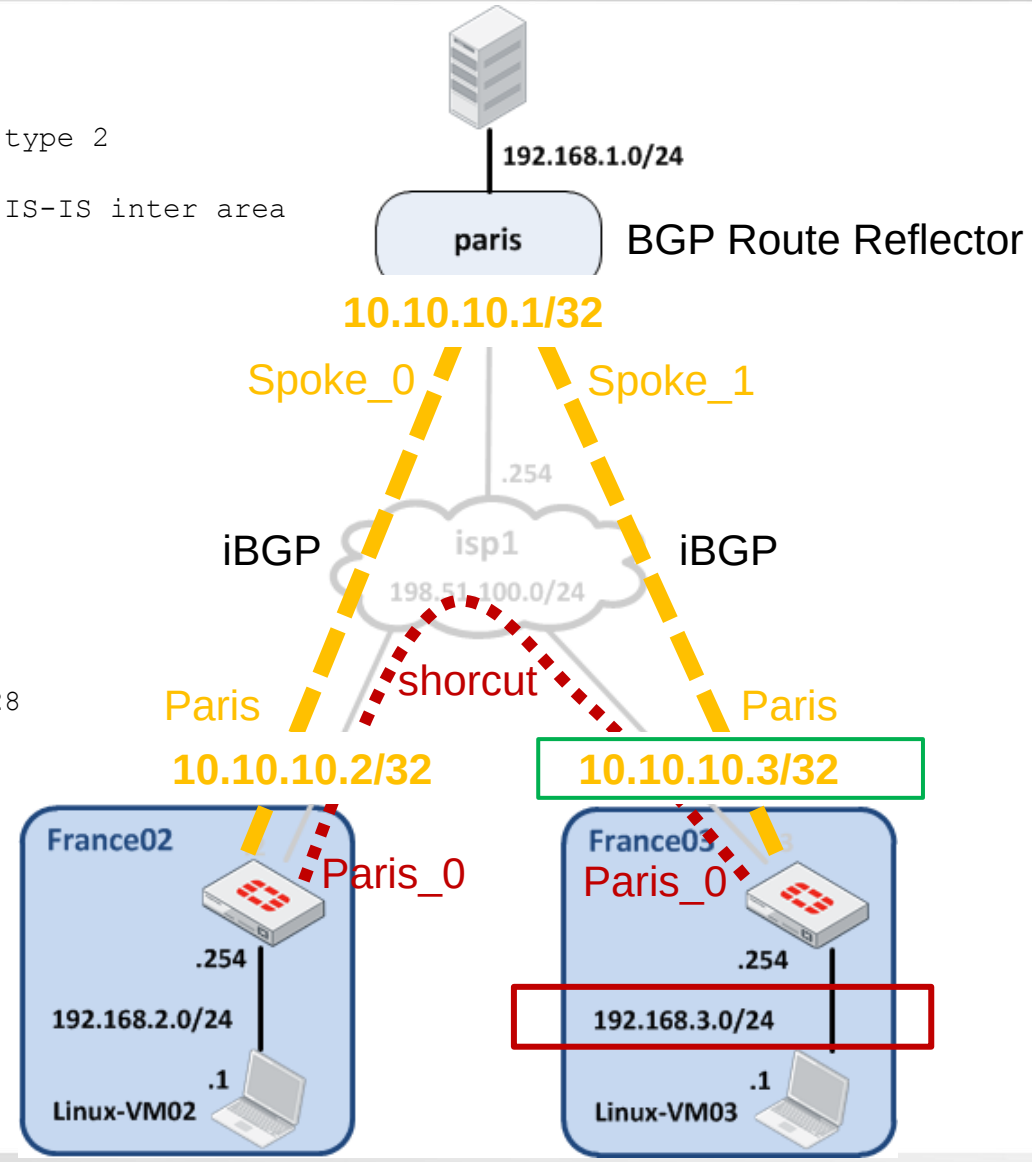
```
France02 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 198.51.100.254, wan1

S       10.10.10.0/24 [10/0] via 10.10.10.1, Paris

C       10.10.10.1/32 is directly connected, Paris
C       10.10.10.2/32 is directly connected, Paris
                      is directly connected, Paris_0
C       10.10.10.3/32 is directly connected, Paris_0

B       192.168.1.0/24 [200/0] via 10.10.10.1, Paris, 02:38:15
C       192.168.2.0/24 is directly connected, internal
B       192.168.3.0/24 [200/0] via 10.10.10.3, Paris_0, 00:00:28

C       198.51.100.0/24 is directly connected, wan1
```



The BGP Next-Hop of France03 is now directly connected

With shortcut – RIB lookup

```
France02 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 198.51.100.254, wan1

S       10.10.10.0/24 [10/0] via 10.10.10.1, Paris

C       10.10.10.1/32 is directly connected, Paris
C       10.10.10.2/32 is directly connected, Paris
                      is directly connected, Paris_0
C       10.10.10.3/32 is directly connected, Paris_0

B       192.168.1.0/24 [200/0] via 10.10.10.1, Paris, 02:38:15
C       192.168.2.0/24 is directly connected, internal
B       192.168.3.0/24 [200/0] via 10.10.10.3, Paris_0, 00:00:28

C       198.51.100.0/24 is directly connected, wan1
```



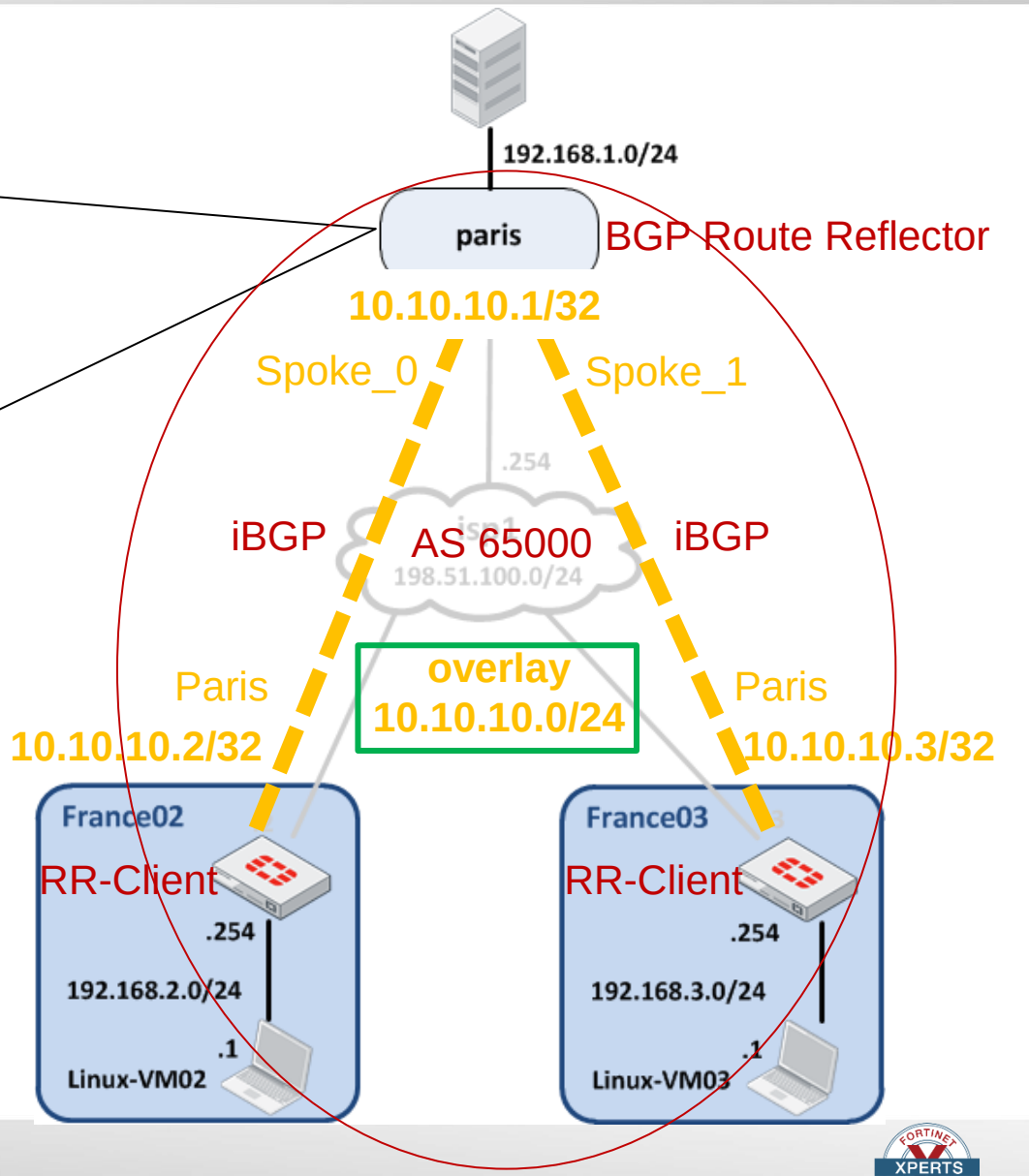
Spoke-to-Spoke traffic flows through the shortcut

ADVPN configuration

BGP configuration

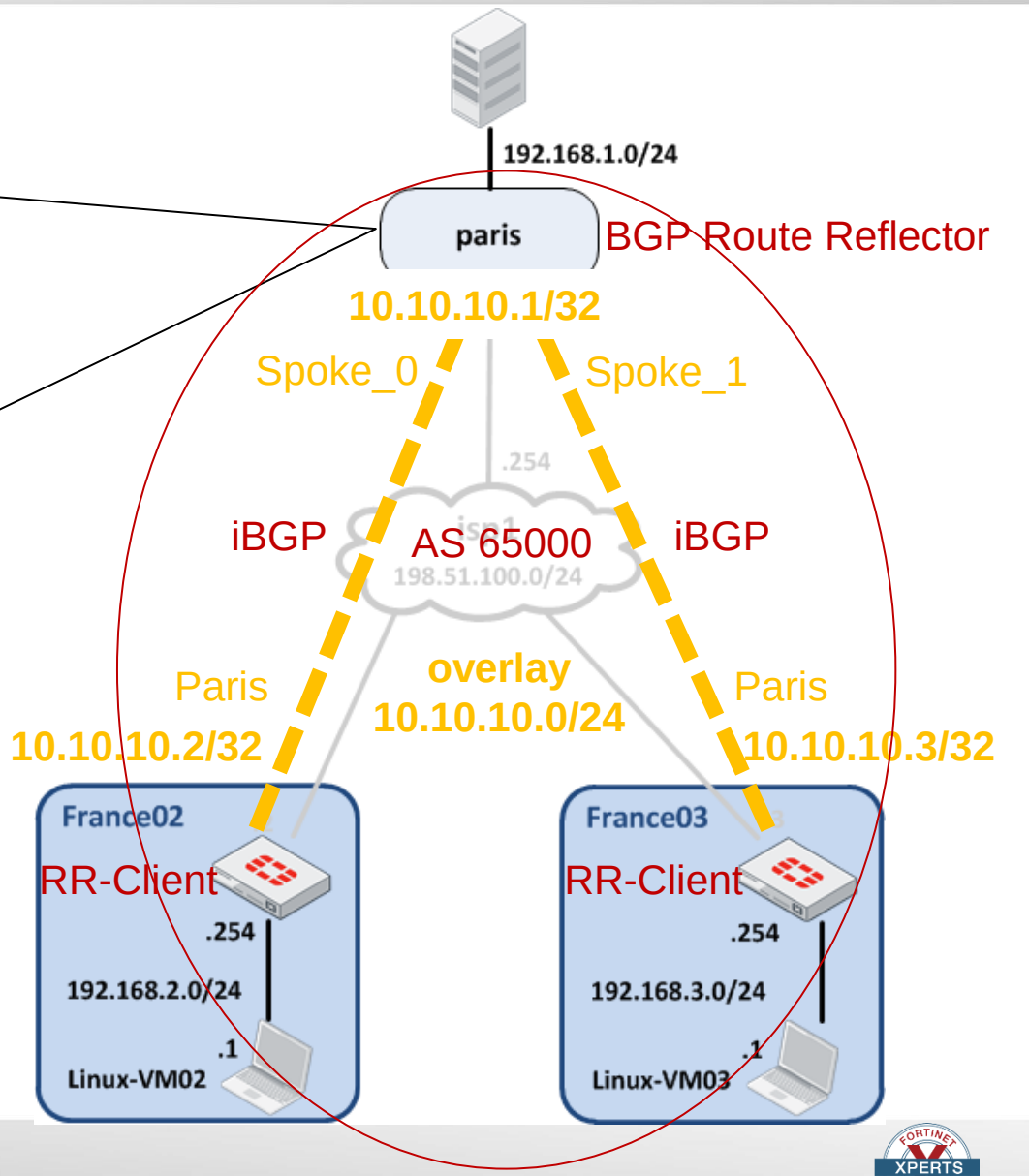
Hub configuration = iBGP Route Reflector (RR)

```
Paris # show router bgp
config router bgp
    set as 65000
    set router-id 10.10.10.1
    config neighbor-group
        edit "advn_peers"
            set remote-as 65000
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.10.0 255.255.255.0
            set neighbor-group "advn_peers"
        next
    end
    config network
        edit 1
            set prefix 192.168.1.0 255.255.255.0
        next
    end
end
```



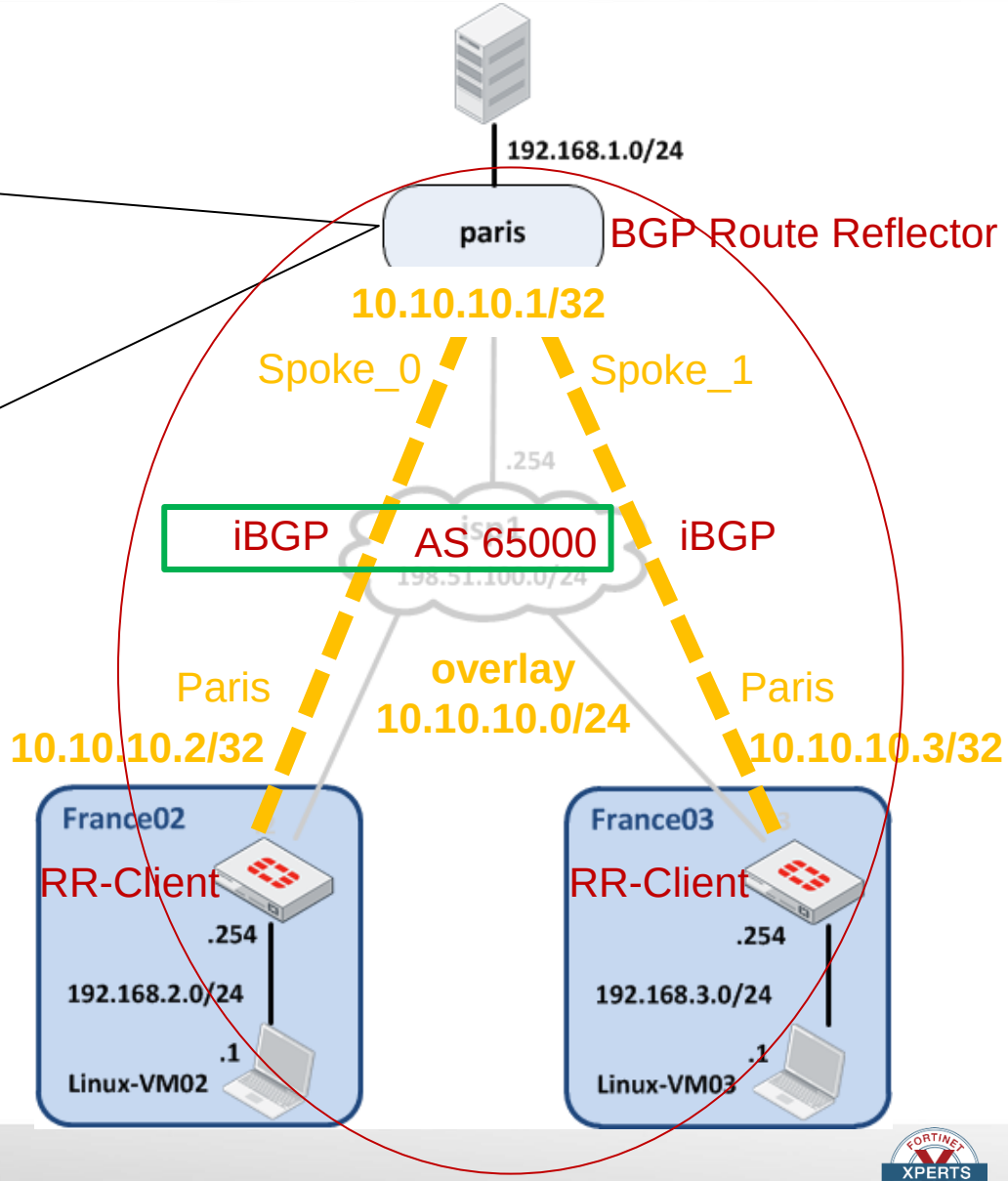
Hub configuration = iBGP Route Reflector (RR)

```
Paris # show router bgp
config router bgp
    set as 65000
    set router-id 10.10.10.1
    config neighbor-group
        edit "advn_peers"
            set remote-as 65000
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.10.0 255.255.255.0
            set neighbor-group "advn_peers"
        next
    end
    config network
        edit 1
            set prefix 192.168.1.0 255.255.255.0
        next
    end
end
```



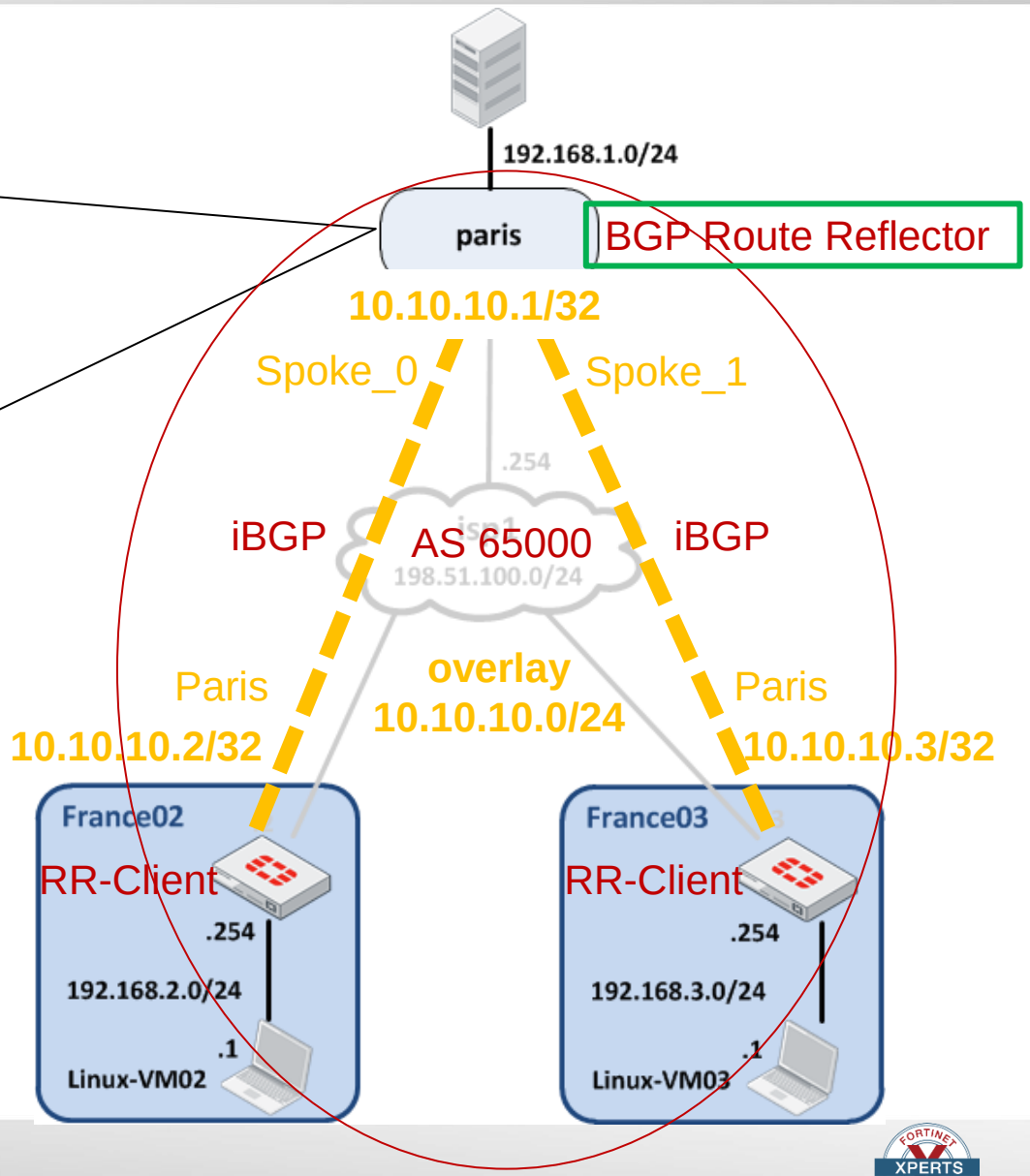
Hub configuration = iBGP Route Reflector (RR)

```
Paris # show router bgp
config router bgp
    set as 65000
    set router-id 10.10.10.1
    config neighbor-group
        edit "advn_peers"
            set remote-as 65000
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.10.0 255.255.255.0
            set neighbor-group "advn_peers"
        next
    end
    config network
        edit 1
            set prefix 192.168.1.0 255.255.255.0
        next
    end
end
```



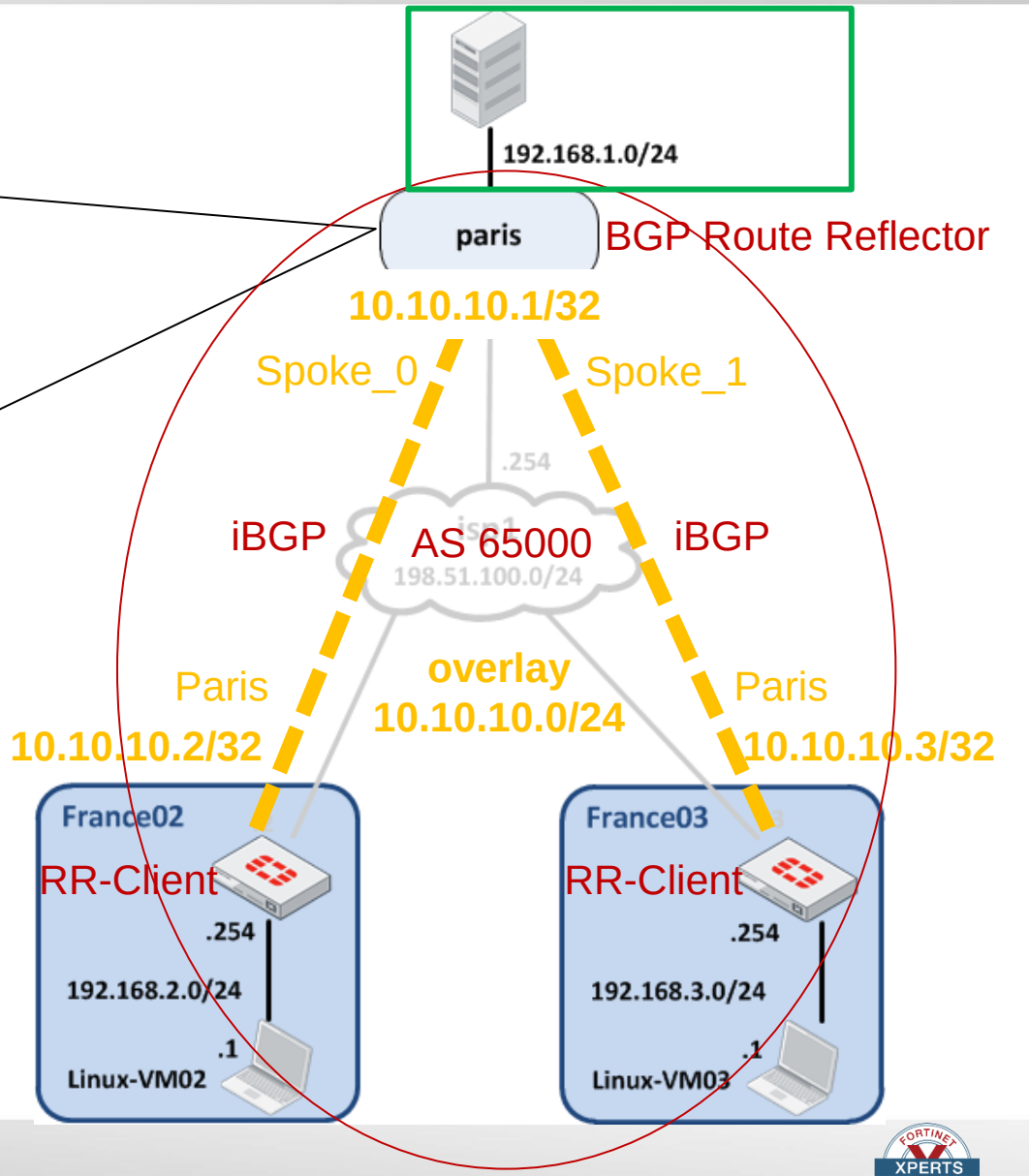
Hub configuration = iBGP Route Reflector (RR)

```
Paris # show router bgp
config router bgp
    set as 65000
    set router-id 10.10.10.1
    config neighbor-group
        edit "advn_peers"
            set remote-as 65000
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.10.0 255.255.255.0
            set neighbor-group "advn_peers"
        next
    end
    config network
        edit 1
            set prefix 192.168.1.0 255.255.255.0
        next
    end
end
```



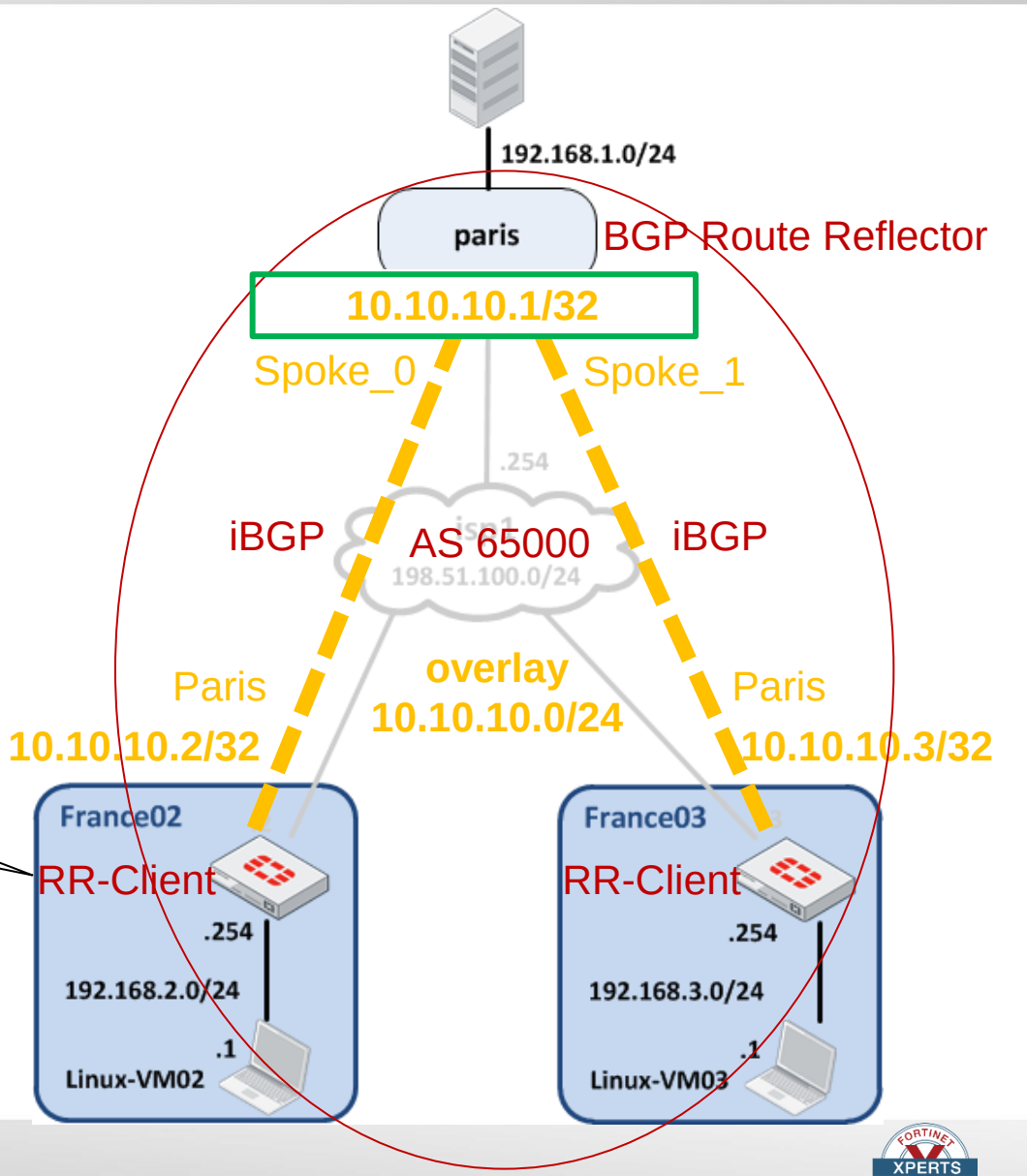
Hub configuration = iBGP Route Reflector (RR)

```
Paris # show router bgp
config router bgp
    set as 65000
    set router-id 10.10.10.1
    config neighbor-group
        edit "advn_peers"
            set remote-as 65000
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.10.0 255.255.255.0
            set neighbor-group "advn_peers"
        next
    end
    config network
        edit 1
            set prefix 192.168.1.0 255.255.255.0
        next
    end
end
```



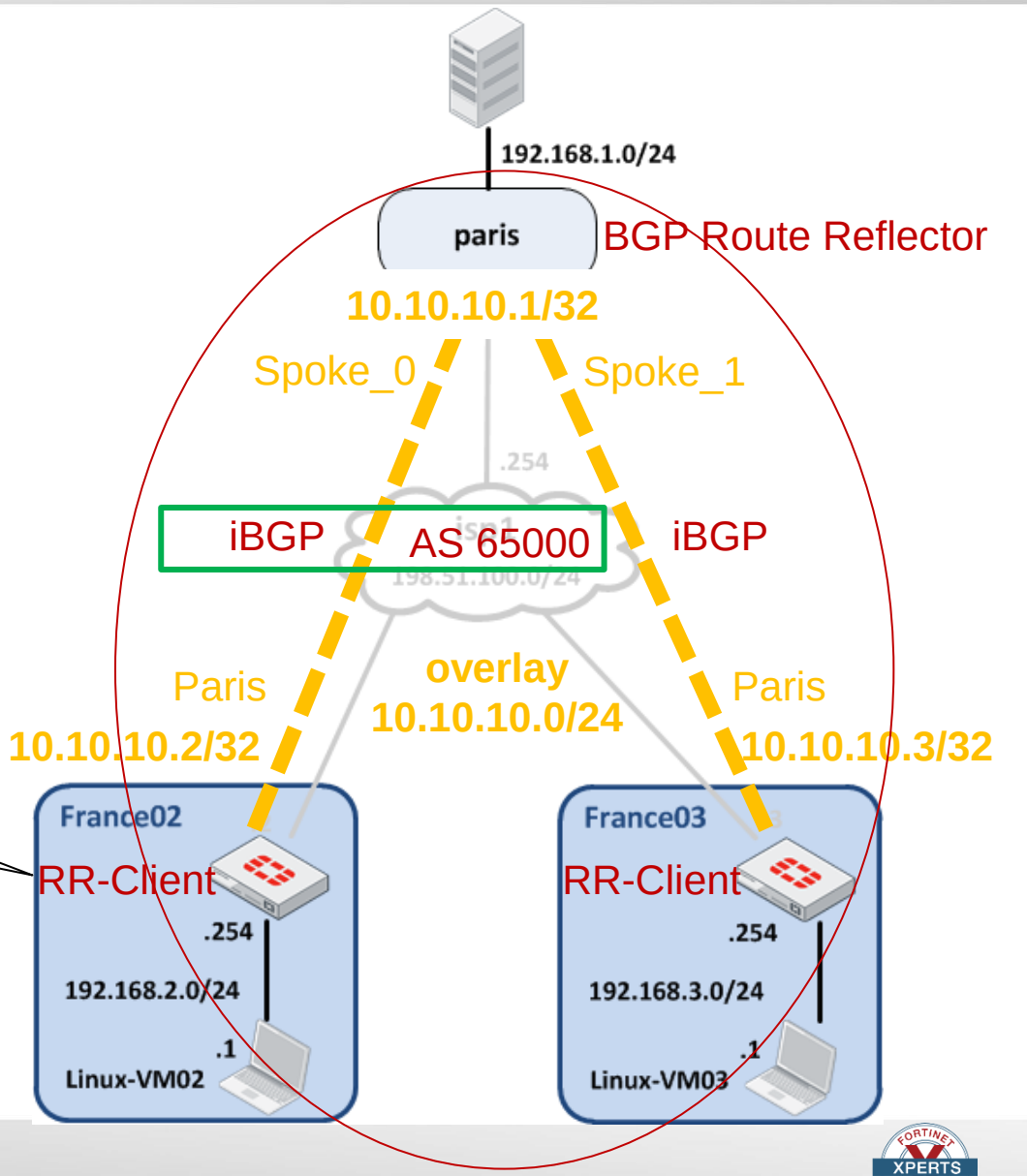
Spoke configuration = iBGP RR-Client

```
France02 # show router bgp
config router bgp
    set as 65000
    set router-id 10.10.10.2
    config neighbor
        edit "10.10.10.1"
            set remote-as 65000
        next
    end
    config network
        edit 1
            set prefix 192.168.2.0 255.255.255.0
        next
    end
end
```



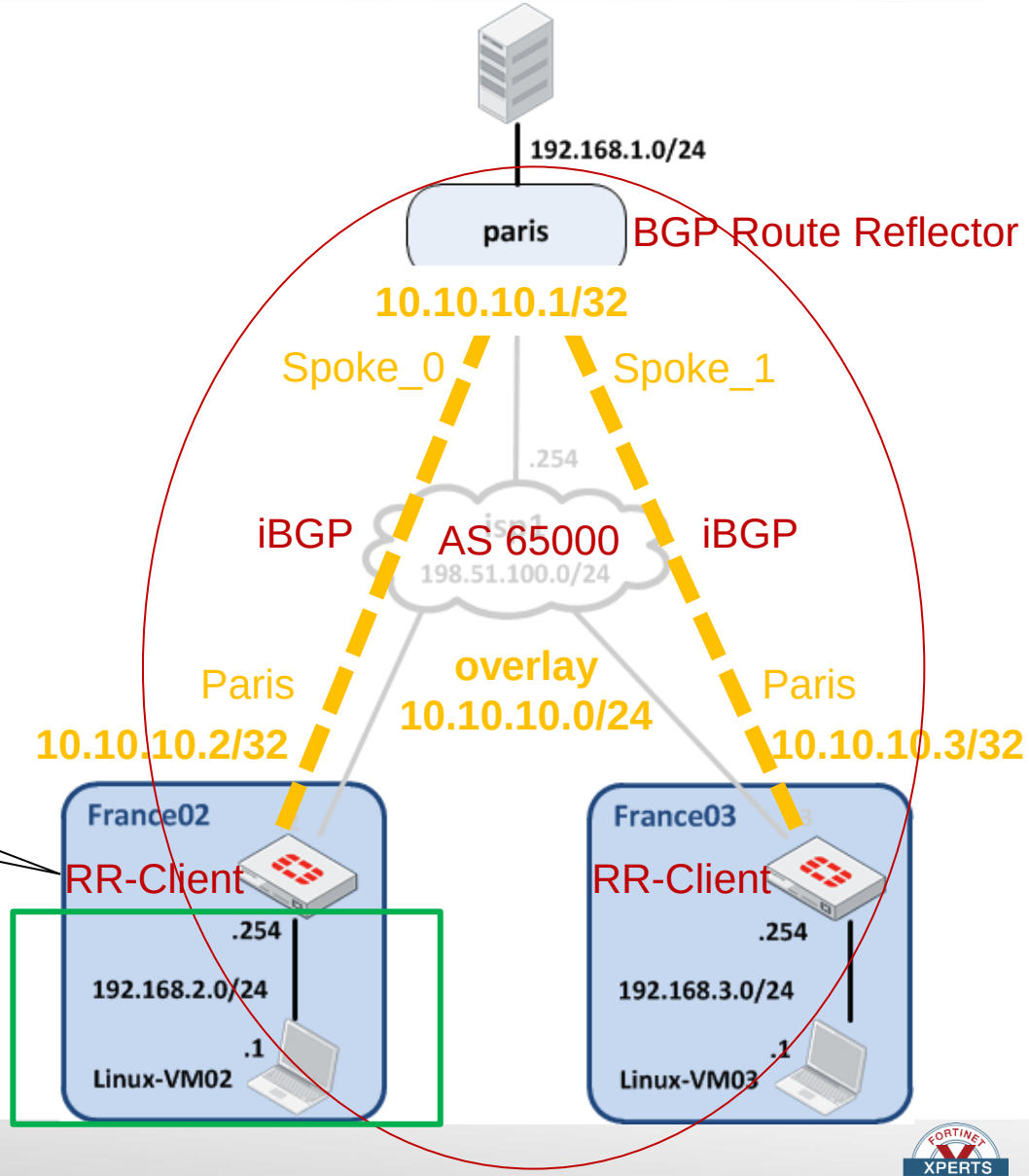
Spoke configuration = iBGP RR-Client

```
France02 # show router bgp
config router bgp
    set as 65000
    set router-id 10.10.10.2
    config neighbor
        edit "10.10.10.1"
            set remote-as 65000
        next
    end
    config network
        edit 1
            set prefix 192.168.2.0 255.255.255.0
        next
    end
end
```



Spoke configuration = iBGP RR-Client

```
France02 # show router bgp
config router bgp
    set as 65000
    set router-id 10.10.10.2
    config neighbor
        edit "10.10.10.1"
            set remote-as 65000
        next
    end
    config network
        edit 1
            set prefix 192.168.2.0 255.255.255.0
        next
    end
end
```



Useful CLI commands

IPsec

Useful CLI commands – IPsec

```
France02 # diag ip address list
<...>
IP=10.10.10.2->10.10.10.1/255.255.255.255 index=15 devname=Paris
<...>
```

overlay `local-ip` and `remote-ip`

List of IP addresses

```
France02 # diag vpn ike gateway list

vd: root/0
name: Paris
version: 1
interface: port2 4
addr: 198.51.100.2:500 -> 198.51.100.1:500
virtual-interface-addr: 10.10.10.2 -> 10.10.10.1
created: 231s ago
auto-discovery: 2 receiver
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 18 4886536f45c96972/07719003173cab1d
  direction: initiator
  status: established 231-231s ago = 0ms
  proposal: aes128-sha1
  key: 9ae438a4e65febe2-ad76a0143b49344b
  lifetime/rekey: 86400/85868
  DPD sent/recv: 00000000/00000000
```

List all the IKE SA (“phase1 up”)

Useful CLI commands – IPsec

```
France02 # diag vpn tunnel list
list all ipsec tunnel in vd 0
-----------------------------------------------------
name=Paris ver=1 serial=1 198.51.100.2:0->198.51.100.1:0
bound_if=4 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refcnt=21 ilast=1 olast=1 auto-discovery=2
stat: rxp=63 txp=58 rxb=8424 txb=3627
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=Paris proto=0 sa=1 ref=2 serial=1 adr
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42941/0B replaywin=2048 seqno=3b esn=0 replaywin_lastseq=00000040
  life: type=01 bytes=0/0 timeout=43172/43200
  dec: spi=8135a40e esp=aes key=16 97e4ad16da7bb2a3880b65311da8e50e
       ah=sha1 key=20 968a42ff561c7ea5fd4d8a94546c09f4812f0dcf
  enc: spi=e77918f5 esp=aes key=16 0143920846bd2087bb56250e855a4352
       ah=sha1 key=20 328d6e7713f2beb8d44ec4944ca868258236c812
  dec:pkts/bytes=63/4278, enc:pkts/bytes=58/7488
```

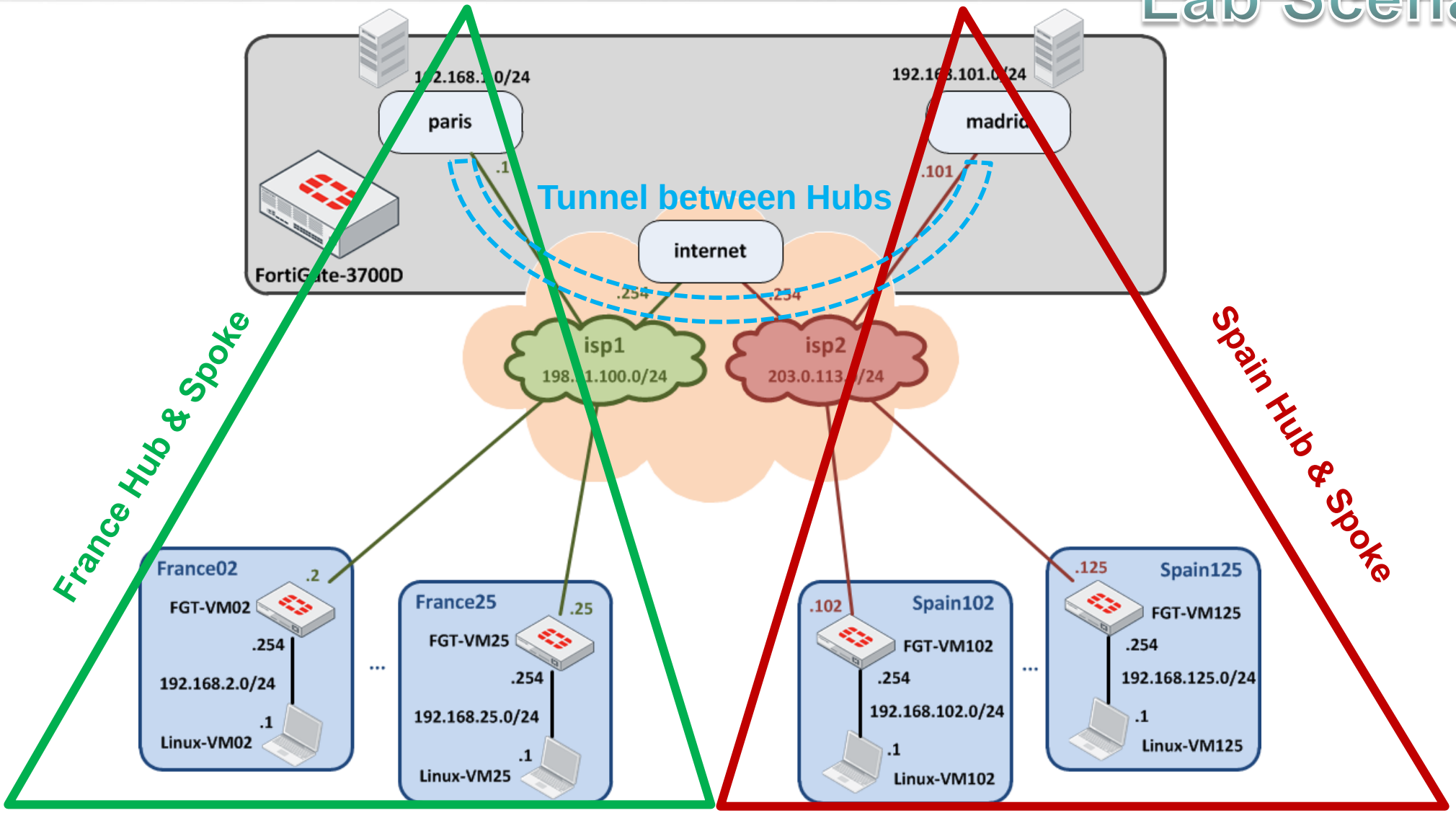
List all the IPsec SA (“phase2/tunnel up”)

```
France02 # get vpn ipsec tunnel summary
'Paris' 198.51.100.1:0  selectors(total,up): 1/1  rx(pkt,err): 66/0  tx(pkt,err): 60/0
```

```
France02 # diag vpn ike status detailed
vd: root/0
name: Paris
version: 1
connection: 1/12
IKE SA: created 1/19  established 1/19  times 0/2/10 ms
IPsec SA: created 1/27  established 1/27  times 0/1/10 ms
```

Hub & Spoke Architecture

Xpert Academy
Lab Scenario



Useful CLI commands – IPsec

```
[root:~]# ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1): 56 data bytes
64 bytes from 192.168.3.1: icmp_seq=0 ttl=252 time=1.1 ms
64 bytes from 192.168.3.1: icmp_seq=1 ttl=253 time=0.6 ms
64 bytes from 192.168.3.1: icmp_seq=2 ttl=253 time=0.5 ms
64 bytes from 192.168.3.1: icmp_seq=3 ttl=253 time=0.3 ms
64 bytes from 192.168.3.1: icmp_seq=4 ttl=253 time=0.4 ms

--- 192.168.3.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.5/1.1 ms
```

Ping from France02 LAN to France03 LAN

```
France02 # get vpn ipsec tunnel summary
'Paris_0' 198.51.100.3:0  selectors(total,up): 1/1  rx(pkt,err): 6/0  tx(pkt,err): 6/0
'Paris' 198.51.100.1:0  selectors(total,up): 1/1  rx(pkt,err): 125/0  tx(pkt,err): 113/0
```

Shortcut to France03

```
[root:~]# ping 192.168.102.1
PING 192.168.102.1 (192.168.102.1): 56 data bytes
64 bytes from 192.168.102.1: icmp_seq=0 ttl=251 time=1.8 ms
64 bytes from 192.168.102.1: icmp_seq=1 ttl=253 time=0.7 ms
64 bytes from 192.168.102.1: icmp_seq=2 ttl=253 time=0.7 ms
64 bytes from 192.168.102.1: icmp_seq=3 ttl=253 time=0.8 ms
64 bytes from 192.168.102.1: icmp_seq=4 ttl=253 time=0.7 ms

--- 192.168.102.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.7/0.9/1.8 ms
```

Ping from France02 LAN to Spain102 LAN

```
France02 # get vpn ipsec tunnel summary
'Paris_0' 198.51.100.3:0  selectors(total,up): 1/1  rx(pkt,err): 7/0  tx(pkt,err): 7/0
'Paris_1' 203.0.113.102:0  selectors(total,up): 1/1  rx(pkt,err): 5/0  tx(pkt,err): 5/0
'Paris' 198.51.100.1:0  selectors(total,up): 1/1  rx(pkt,err): 134/0  tx(pkt,err): 121/0
```

Shortcut to Spain102

Useful CLI commands – IPsec

```
[root:~]# ping 192.168.101.1
PING 192.168.101.1 (192.168.101.1): 56 data bytes
64 bytes from 192.168.101.1: icmp_seq=0 ttl=252 time=1.1 ms
64 bytes from 192.168.101.1: icmp_seq=1 ttl=253 time=0.8 ms
64 bytes from 192.168.101.1: icmp_seq=2 ttl=253 time=0.7 ms
64 bytes from 192.168.101.1: icmp_seq=3 ttl=253 time=0.7 ms
64 bytes from 192.168.101.1: icmp_seq=4 ttl=253 time=0.5 ms

--- 192.168.101.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.7/1.1 ms
```

Ping from France02 LAN to Madrid LAN

```
France02 # get vpn ipsec tunnel summary
'Paris_0' 198.51.100.3:0  selectors(total,up): 1/1  rx(pkt,err): 8/0  tx(pkt,err): 10/0
'Paris_1' 203.0.113.102:0  selectors(total,up): 1/1  rx(pkt,err): 7/0  tx(pkt,err): 8/0
'Paris_2' 203.0.113.1:0  selectors(total,up): 1/1  rx(pkt,err): 5/0  tx(pkt,err): 5/0
'Paris' 198.51.100.1:0  selectors(total,up): 1/1  rx(pkt,err): 144/0  tx(pkt,err): 130/0
```

Shortcut to Madrid

```
France02 # diag ip address list
<...>
IP=10.10.10.2->10.10.10.1/255.255.255.255 index=15 devname=Paris
IP=10.10.10.2->10.10.10.3/255.255.255.255 index=39 devname=Paris_0
IP=10.10.10.2->10.20.20.2/255.255.255.255 index=40 devname=Paris_1
IP=10.10.10.2->10.255.255.2/255.255.255.255 index=41 devname=Paris_2
<...>
```

Useful CLI commands – IPsec

```
France02 # diag vpn ike status detailed
vd: root/0
name: Paris
version: 1
used-indices: 0-2
connection: 4/15
IKE SA: created 4/22  established 4/22  times 0/2/10 ms
IPsec SA: created 4/30  established 4/30  times 0/1/10 ms

France02 # diag netlink interface list
<...>
if=Paris family=00 type=768 index=15 mtu=1438 link=0 master=0
ref=24 state=off start fw_flags=0 flags=up p2p run noarp multicast

if=Paris_0 family=00 type=768 index=39 mtu=1438 link=15 master=0
ref=21 state=off start fw_flags=0 flags=up p2p run noarp multicast

if=Paris_1 family=00 type=768 index=40 mtu=1438 link=15 master=0
ref=21 state=off start fw_flags=0 flags=up p2p run noarp multicast

if=Paris_2 family=00 type=768 index=41 mtu=1438 link=15 master=0
ref=25 state=off start fw_flags=0 flags=up p2p run noarp multicast
<...>
```

List of IPsec interfaces

Bring down a shortcut

```
France02 # diag vpn ike gateway flush name Paris_2

France02 # get vpn ipsec tunnel summary
'Paris_0' 198.51.100.3:0  selectors(total,up): 1/1  rx(pkt,err): 8/0  tx(pkt,err): 10/0
'Paris_1' 203.0.113.102:0  selectors(total,up): 1/1  rx(pkt,err): 7/0  tx(pkt,err): 8/0
'Paris' 198.51.100.1:0  selectors(total,up): 1/1  rx(pkt,err): 144/0  tx(pkt,err): 130/0
```

Shortcuts cannot be flushed via the GUI, use the CLI

Useful CLI commands – IPsec

Debugging an IKE negotiation:

```
diag debug console timestamp enable
diag vpn ike log filter clear
diag vpn ike log filter dst-addr4 X.X.X.X        # replace X.X.X.X with the public IP of the peer
diag debug application ike -1
diag debug application fnbamd -1                 # only if signature authentication or Xauth/EAP is used
diag debug enable
```

Useful CLI commands

Routing

Useful CLI commands – Routing

```
France02 # get router info bgp summary
BGP router identifier 10.10.10.2, local AS number 65000
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.1      4      65000    2061    2049        2    0    0 00:00:23        4

Total number of neighbors 1
```

BGP peers

```
France02 # get router info bgp network
BGP table version is 2, local router ID is 10.10.10.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i192.168.1.0      10.10.10.1               0    100      0 i
*> 192.168.2.0      0.0.0.0                       100  32768 i
*>i192.168.3.0      10.10.10.3               0    100      0 i
*>i192.168.101.0    10.255.255.2             0    100      0 65100 i
*>i192.168.102.0    10.20.20.2               0    100      0 65100 i

Total number of prefixes 5
```

BGP table

Useful CLI commands – Routing

```
France02 # get router info bgp network 192.168.102.0
BGP routing table entry for 192.168.102.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  65100
    10.20.20.2 from 10.10.10.1 (10.10.10.1)
      Origin IGP metric 0, localpref 100, valid, internal, best
      Last update: Tue Jun 21 17:03:02 2016
```

BGP details of a specific prefix

```
France02 # get router info routing-table bgp
B       192.168.1.0/24 [200/0] via 10.10.10.1, Paris, 00:01:03
B       192.168.3.0/24 [200/0] via 10.10.10.3 (recursive via 10.10.10.1), 00:01:03
B       192.168.101.0/24 [200/0] via 10.255.255.2 (recursive via 10.10.10.1), 00:01:03
B       192.168.102.0/24 [200/0] via 10.20.20.2 (recursive via 10.10.10.1), 00:01:03
```

BGP routes in the RIB

```
France02 # get router info routing-table static
S*      0.0.0.0/0 [10/0] via 198.51.100.254, port2
S       10.10.10.0/24 [10/0] via 10.10.10.1, Paris
S       10.20.20.0/24 [10/0] via 10.10.10.1, Paris
S       10.255.255.0/30 [10/0] via 10.10.10.1, Paris
```

Static routes in the RIB

```
France02 # get router info routing-table connected
C       10.5.48.0/20 is directly connected, port10
C       10.10.10.1/32 is directly connected, Paris
C       10.10.10.2/32 is directly connected, Paris
C       192.168.2.0/24 is directly connected, port1
C       198.51.100.0/24 is directly connected, port2
```

Connected routes in the RIB

Useful CLI commands – Routing

```
France02 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 198.51.100.254, port2
C       10.5.48.0/20 is directly connected, port10
S       10.10.10.0/24 [10/0] via 10.10.10.1, Paris
C       10.10.10.1/32 is directly connected, Paris
C       10.10.10.2/32 is directly connected, Paris
S       10.20.20.0/24 [10/0] via 10.10.10.1, Paris
R       10.255.255.0/24 [120/2] via 10.10.10.1, Paris, 00:02:14
S       10.255.255.0/30 [10/0] via 10.10.10.1, Paris
B       192.168.1.0/24 [200/0] via 10.10.10.1, Paris, 00:01:08
C       192.168.2.0/24 is directly connected, port1
B       192.168.3.0/24 [200/0] via 10.10.10.3 (recursive via 10.10.10.1), 00:01:08
B       192.168.101.0/24 [200/0] via 10.255.255.2 (recursive via 10.10.10.1), 00:01:08
B       192.168.102.0/24 [200/0] via 10.20.20.2 (recursive via 10.10.10.1), 00:01:08
C       198.51.100.0/24 is directly connected, port2
```

All active routes in the RIB

```
France02 # get router info routing-table details 192.168.102.1
Routing entry for 192.168.102.0/24
  Known via "bgp", distance 200, metric 0, best
  Last update 00:02:48 ago
  * 10.20.20.2 (recursive via 10.10.10.1)
```

Details of a specific route in the RIB

Useful CLI commands – Routing

```
[root:~]# ping 192.168.3.1
[root:~]# ping 192.168.101.1
[root:~]# ping 192.168.102.1
```

Bring up some shortcuts

```
France02 (root) # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 198.51.100.254, port2
C       10.5.48.0/20 is directly connected, port10
S       10.10.10.0/24 [10/0] via 10.10.10.1, Paris
C       10.10.10.1/32 is directly connected, Paris
C       10.10.10.2/32 is directly connected, Paris
                      is directly connected, Paris_0
                      is directly connected, Paris_1
                      is directly connected, Paris_2
C       10.10.10.3/32 is directly connected, Paris_0
S       10.20.20.0/24 [10/0] via 10.10.10.1, Paris
C       10.20.20.2/32 is directly connected, Paris_2
S       10.255.255.0/24 [10/0] via 10.10.10.1, Paris
C       10.255.255.2/32 is directly connected, Paris_1
B       192.168.1.0/24 [200/0] via 10.10.10.1, Paris, 00:20:39
C       192.168.2.0/24 is directly connected, port1
B       192.168.3.0/24 [200/0] via 10.10.10.3, Paris_0, 00:01:11
B       192.168.101.0/24 [200/0] via 10.255.255.2, Paris_1, 00:00:11
B       192.168.102.0/24 [200/0] via 10.20.20.2, Paris_2, 00:00:11
C       198.51.100.0/24 is directly connected, port2
```

Overlay `local-ip`

BGP Next-Hop are now directly connected

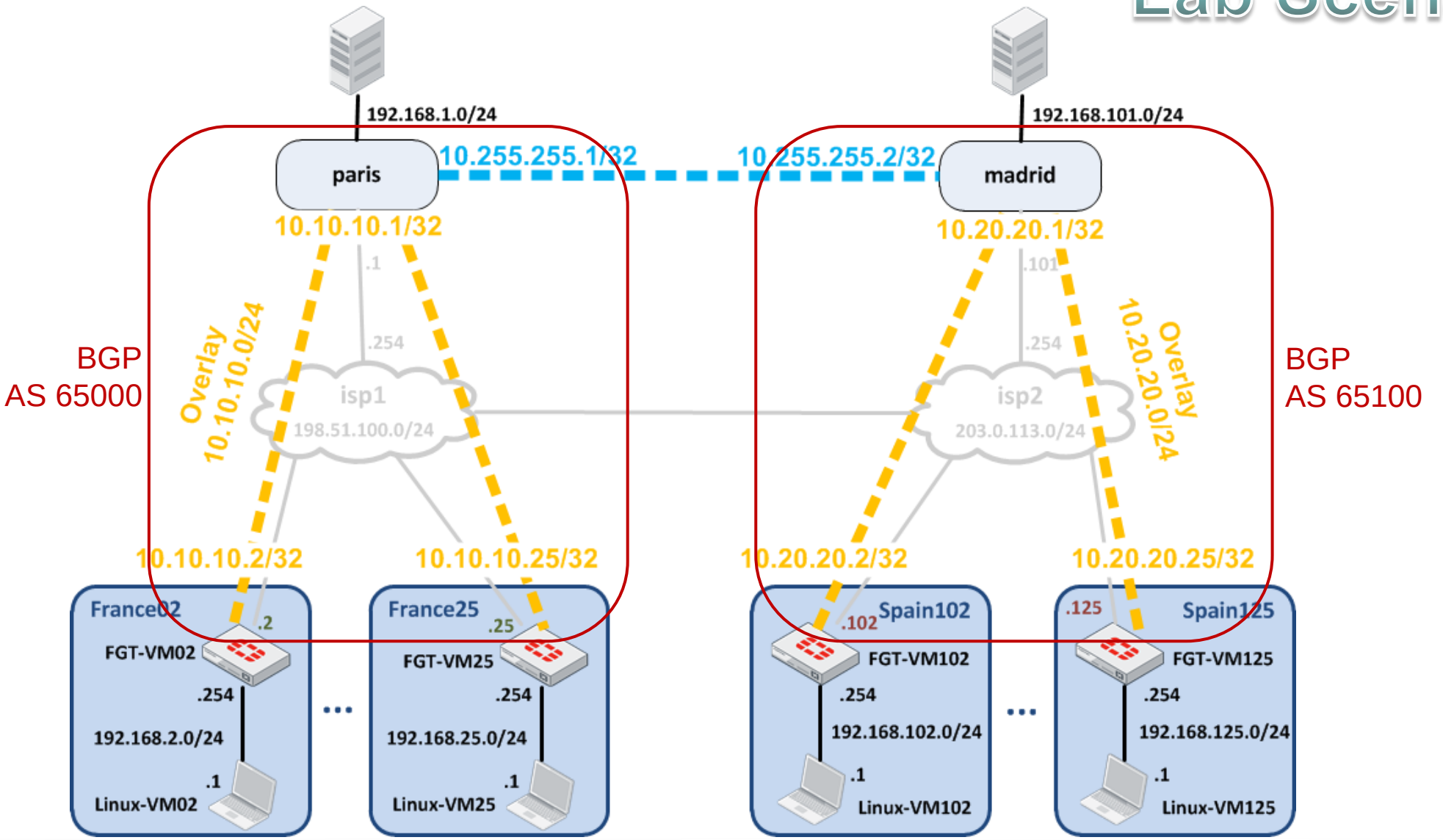
Routes through the shortcuts

ADVPN between two Hub & Spoke

Interconnecting two distinct Hub & Spoke

ADVPN between two distinct Hub & Spoke

Xpert Academy
Lab Scenario



ADVPN between two Hub & Spoke

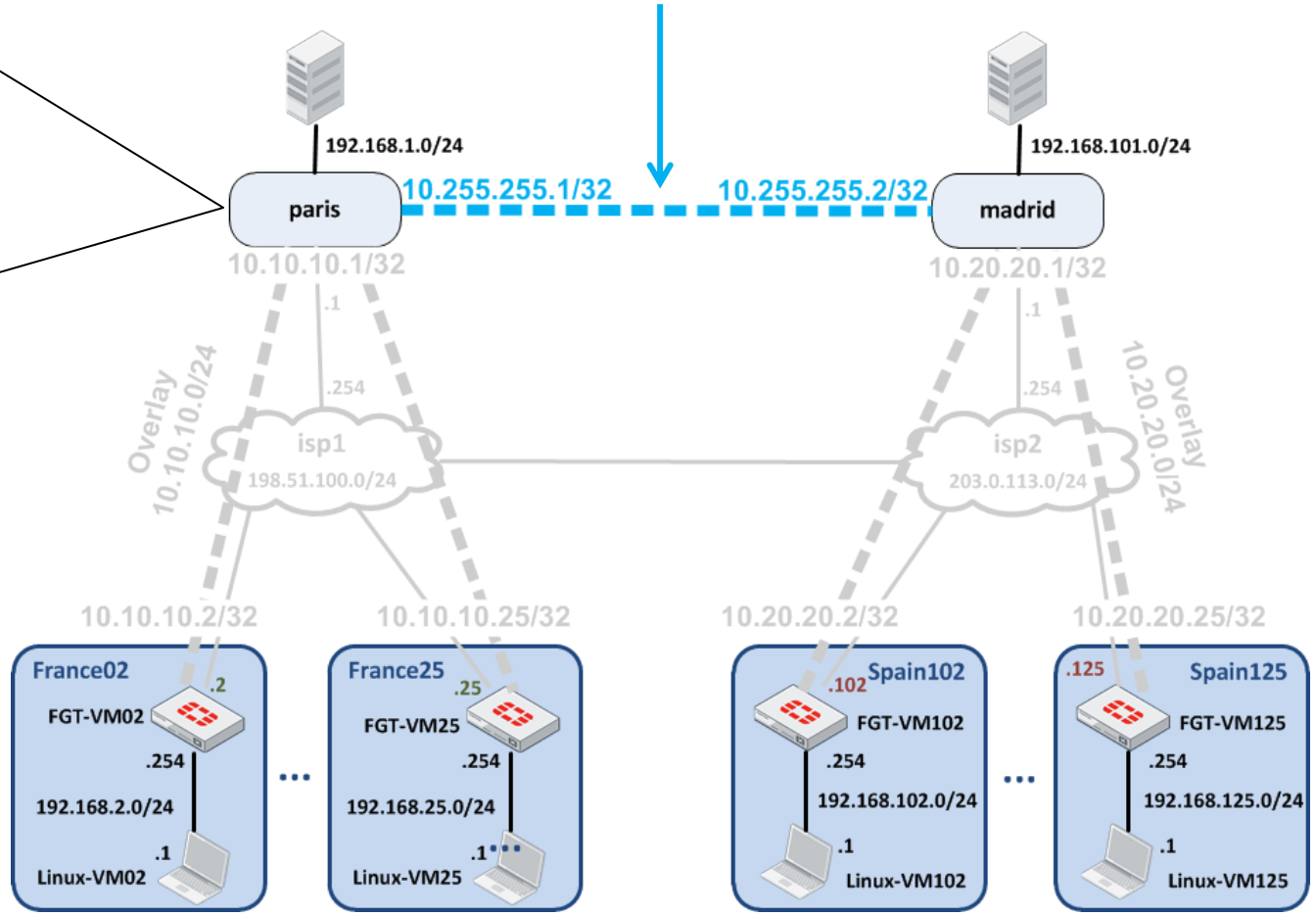
IPsec configuration

ADVPN between two distinct Hub & Spoke

```
config vpn ipsec phase1-interface
    edit "Madrid"
        set interface "port2"
        set proposal aes128-sha1
        set auto-discovery-forwarder enable
        set remote-gw 203.0.113.1
        set psksecret fortinet
    next
end

config vpn ipsec phase2-interface
    edit "Madrid"
        set phase1name "Madrid"
        set proposal aes128-sha1
    next
end

config system interface
    edit "Madrid"
        set ip 10.255.255.1 255.255.255.255
        set remote-ip 10.255.255.2
    next
end

+ Firewall policies:
  . "To Madrid H&S":
    set srcintf "LAN" "Spokes"
    set dstintf "Madrid"

  . "From Madrid H&S":
    set dstintf "LAN" "Spokes"
    set srcintf "Madrid"
```

Requires an IPsec tunnel between the two Hubs

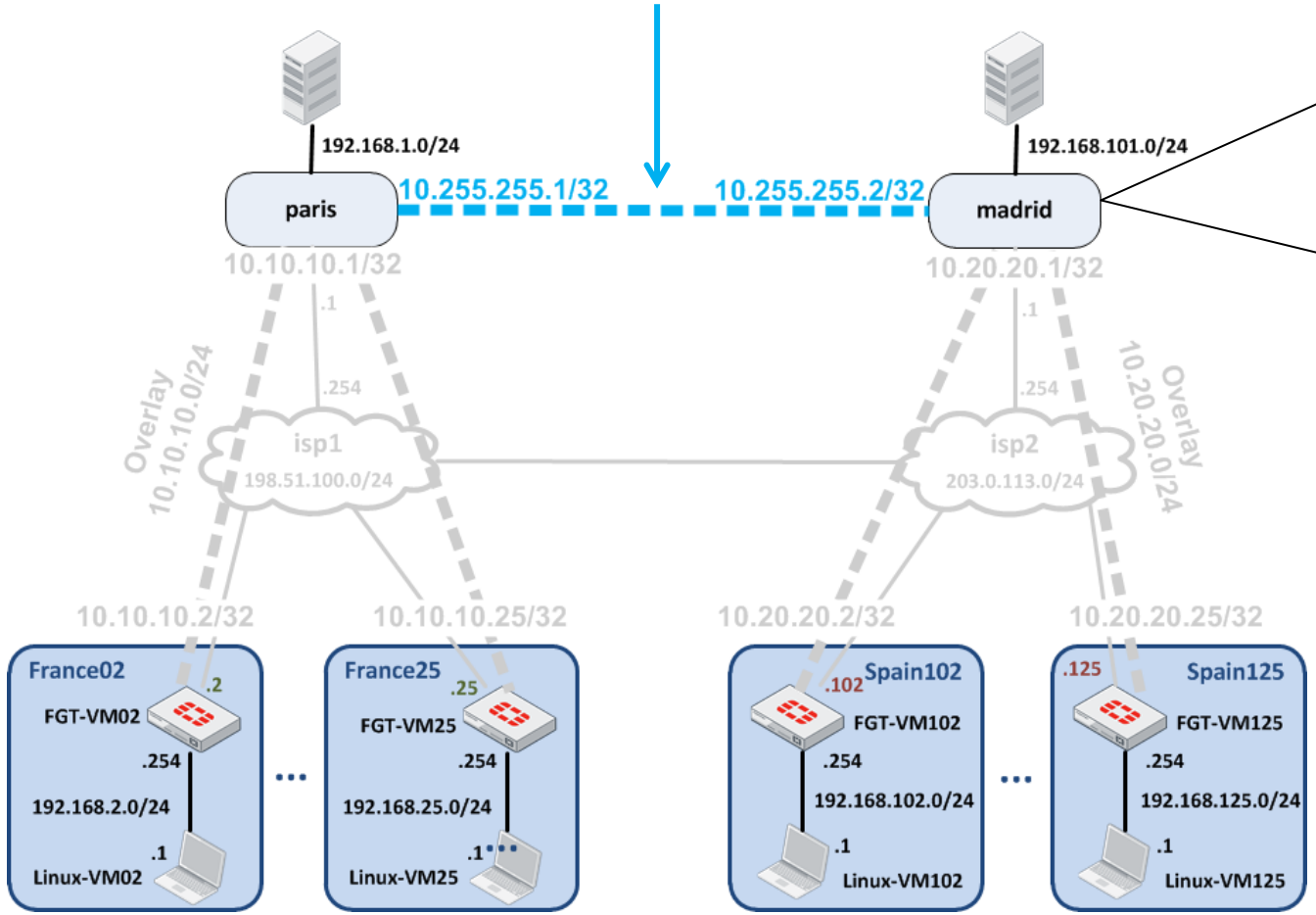
"auto-discovery-forwarder" must be enabled on the Hub-to-Hub tunnel



ADVPN between two distinct Hub & Spoke

Requires an IPsec tunnel between the two Hubs

"`auto-discovery-forwarder`" must be enabled on the Hub-to-Hub tunnel




```
config vpn ipsec phase1-interface
    edit "Paris"
        set interface "port2"
        set proposal aes128-sha1
        set auto-discovery-forwarder enable
        set remote-gw 198.51.100.1
        set psksecret fortinet
    next
end

config vpn ipsec phase2-interface
    edit "Paris"
        set phase1name "Paris"
        set proposal aes128-sha1
    next
end

config system interface
    edit "Paris"
        set ip 10.255.255.2 255.255.255.255
        set remote-ip 10.255.255.1
    next
end

+ Firewall policies:
  . "To Paris H&S":
    set srcintf "LAN" "Spokes"
    set dstintf "Paris"

  . "From Paris H&S":
    set dstintf "LAN" "Spokes"
    set srcintf "Paris"
```

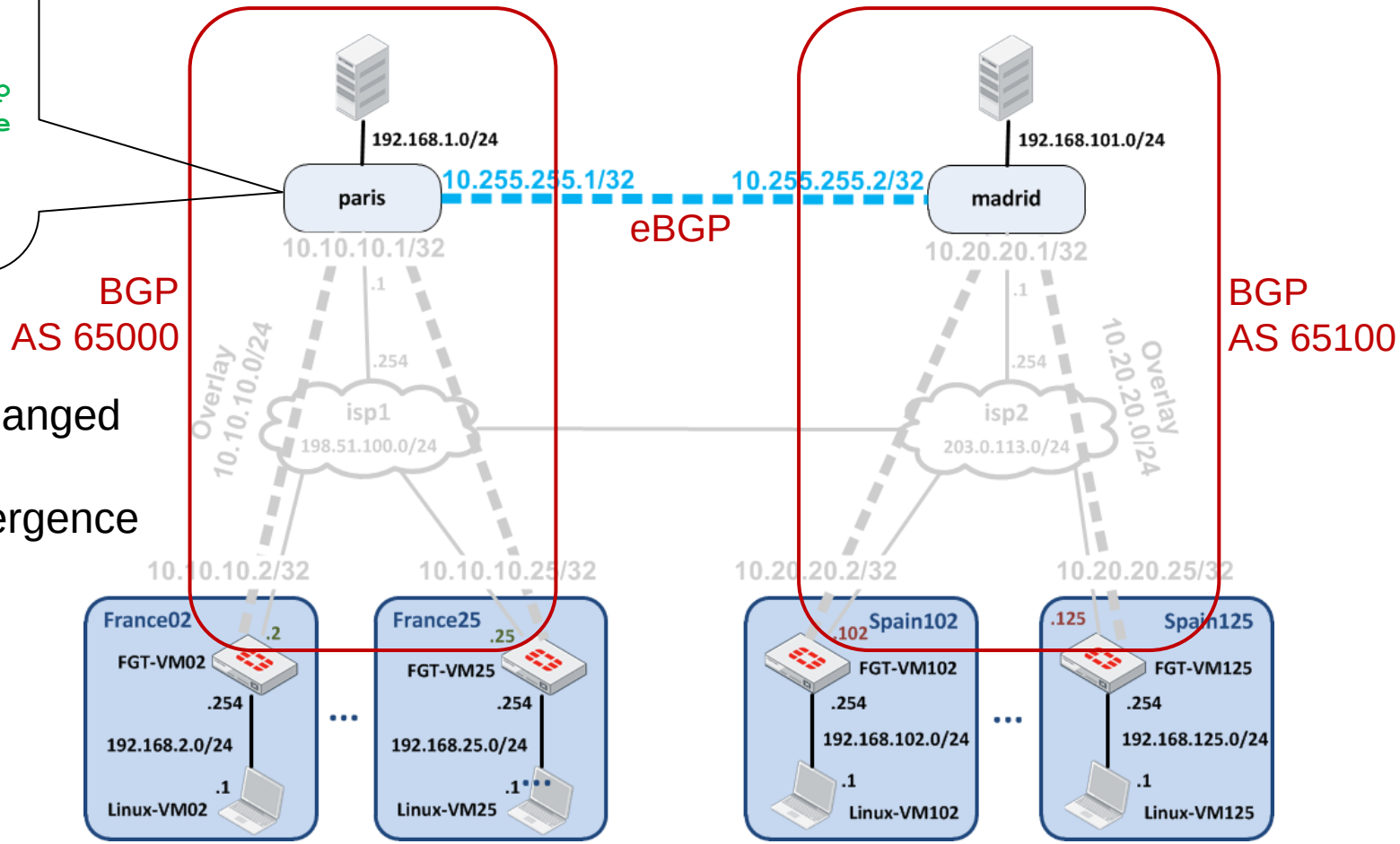
ADVPN between two Hub & Spoke

BGP configuration

ADVPN between two distinct Hub & Spoke

```
config router bgp
    set as 65000
    set router-id 10.10.10.1
    config neighbor
        edit "10.255.255.2"
            set attribute-unchanged next-hop
            set ebgp-enforce-multihop enable
            set remote-as 65100
        next
    end
end
```

eBGP: each Hub & Spoke belongs to a different AS



`attribute-unchanged next-hop`

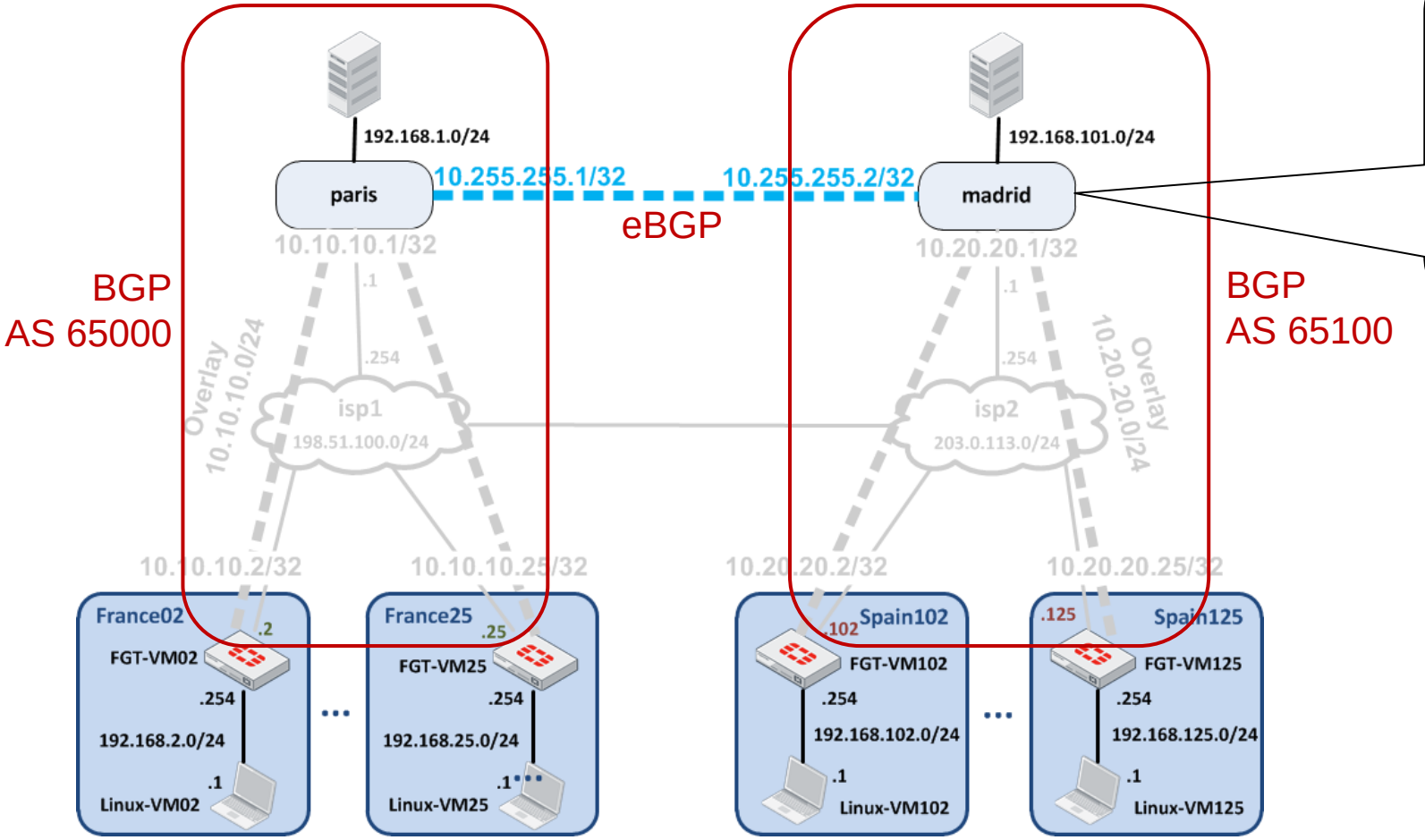
Keep the BGP Next-Hop attributes unchanged when BGP routes exit the AS.
This is mandatory to allow routing convergence over the ADVPN shortcuts.

`ebgp-enforce-multihop`

Is required for next-hop-unchanged

ADVPN between two distinct Hub & Spoke

eBGP: each Hub & Spoke belongs to a different AS




```
config router bgp
    set as 65100
    set router-id 10.20.20.1
    config neighbor
        edit "10.255.255.1"
            set attribute-unchanged next-hop
            set ebgp-enforce-multihop enable
            set remote-as 65000
        next
    end
end
```

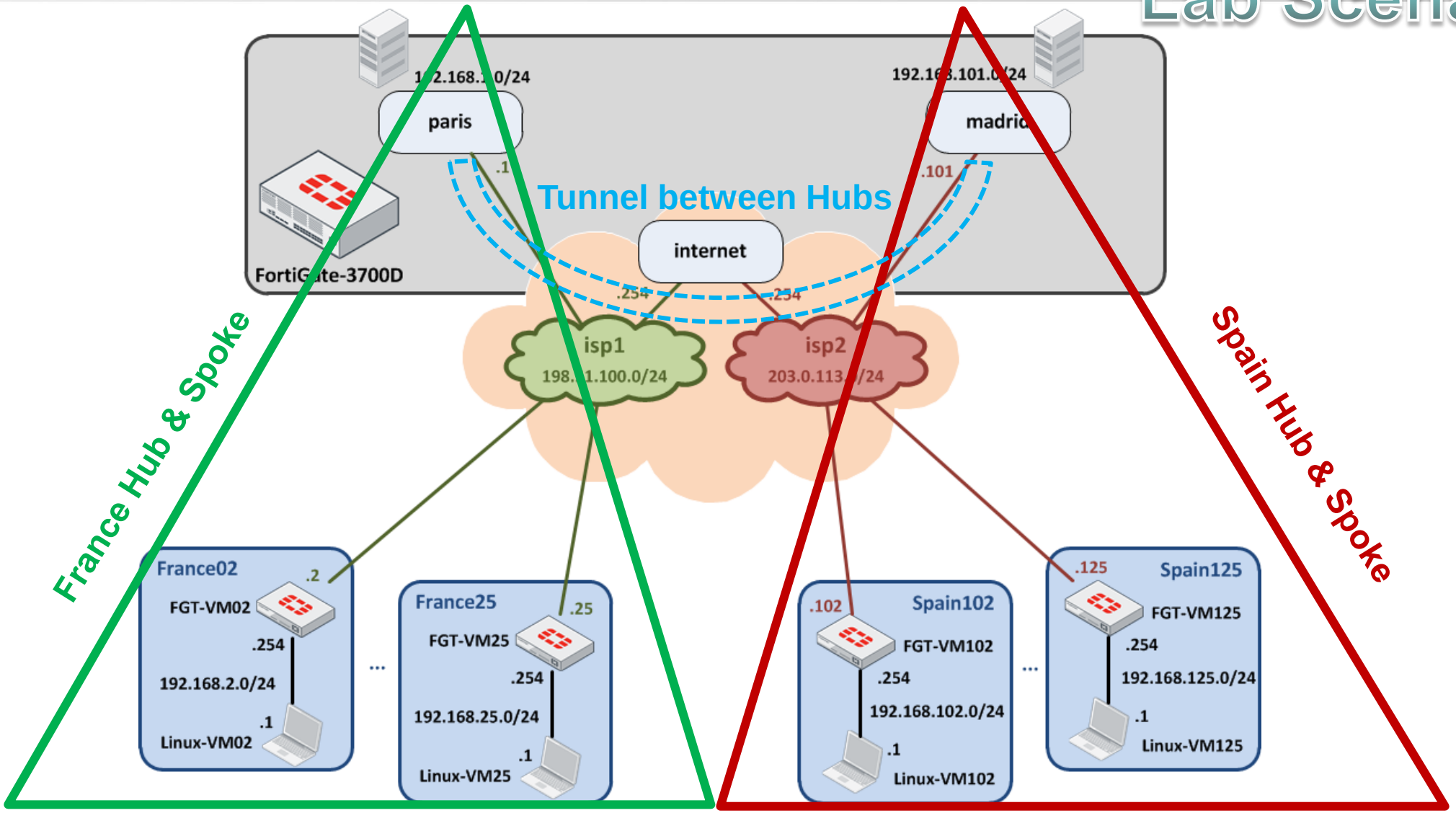
ADVPN Hands-On Experience

ADVPN between two distinct Hub & Spoke

© Copyright Fortinet Inc. All rights reserved.

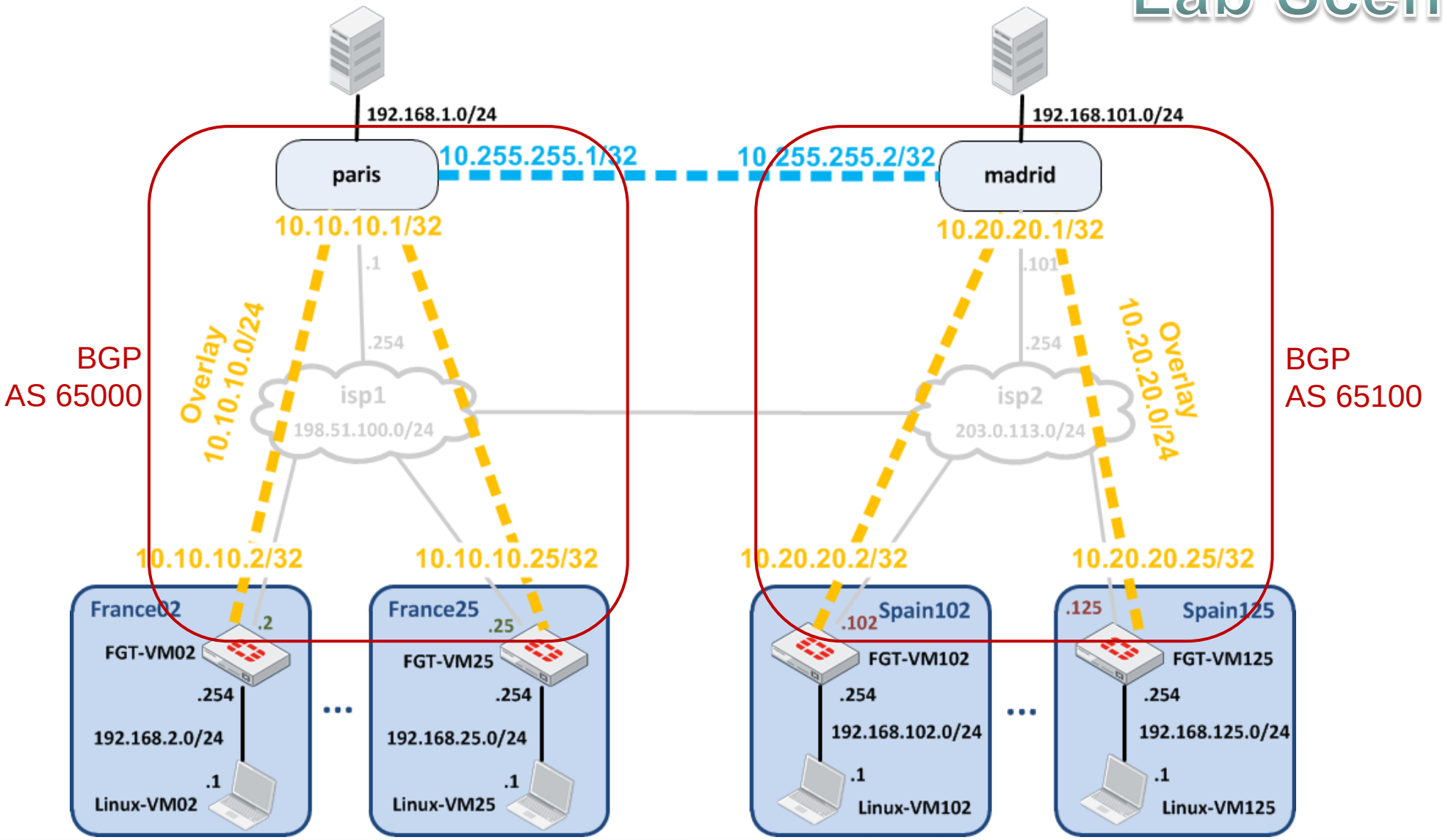
Hub & Spoke Architecture

Xpert Academy
Lab Scenario



Hub & Spoke Overlay Networks

Xpert Academy
Lab Scenario



ADVPN Hands-On Experience

Access to the Linux VMs

http://192.168.45.200/xxx (xxx = VM-id) Google Chrome is recommended

Examples:

- France-05: http://192.168.45.200/005
- Spain-102: http://192.168.45.200/102

Then access the FGT-VM via its internal interface (port1):

ssh admin@192.168.xxx.254 (xxx = VM-id)

Access to "Paris" and "Madrid" Hubs (vdoms) on the FGT-3700D:

- IP: 192.168.45.201
- username: fortinet (read-only account)
- password: fortinet
- management: telnet, ssh, http, https

ADVPN Hands-On Experience

Student-125

192.168.45.200/125

SPICE

Connect to the Linux-VM (here Spain125)

Linux-VM (Use F5 to refresh the window in case of display issue)

Computer

mint's Home

Install Linux Mint

Terminal

File Edit View Search Terminal Help

```
mint@mint ~ $
mint@mint ~ $ ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:df:0d:49
          inet addr:192.168.125.1  Bcast:192.168.125.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:ff:fedf:d49/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14686 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1768 (1.7 KB)  TX bytes:3028808 (3.0 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:26 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1818 (1.8 KB)  TX bytes:1818 (1.8 KB)

mint@mint ~ $
mint@mint ~ $ ssh admin@192.168.125.254
The authenticity of host '192.168.125.254 (192.168.125.254)' can't be established.
ED25519 key fingerprint is aa:41:47:3b:75:98:01:23:48:35:71:83:61:f9:8a:83.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.125.254' (ED25519) to the list of known hosts.
Spain-125 #
Spain-125 #
Spain-125 #
```

Log to the FGT-VM

Menu

Terminal
Use the command line

Fri Jun 24, 11:52

ADVPN Hands-On Experience

Configuration Steps:

1. Create the tunnel towards the Hub (GUI)
2. Configure the overlay IPs on the tunnel interface (GUI)
3. Enable ADVPN on the tunnel (CLI)
4. Create firewall policies (GUI)
5. Configure the static routes for the VPN overlay subnets (GUI)
6. Configure BGP peering with the Hub (GUI)

Validation Steps:

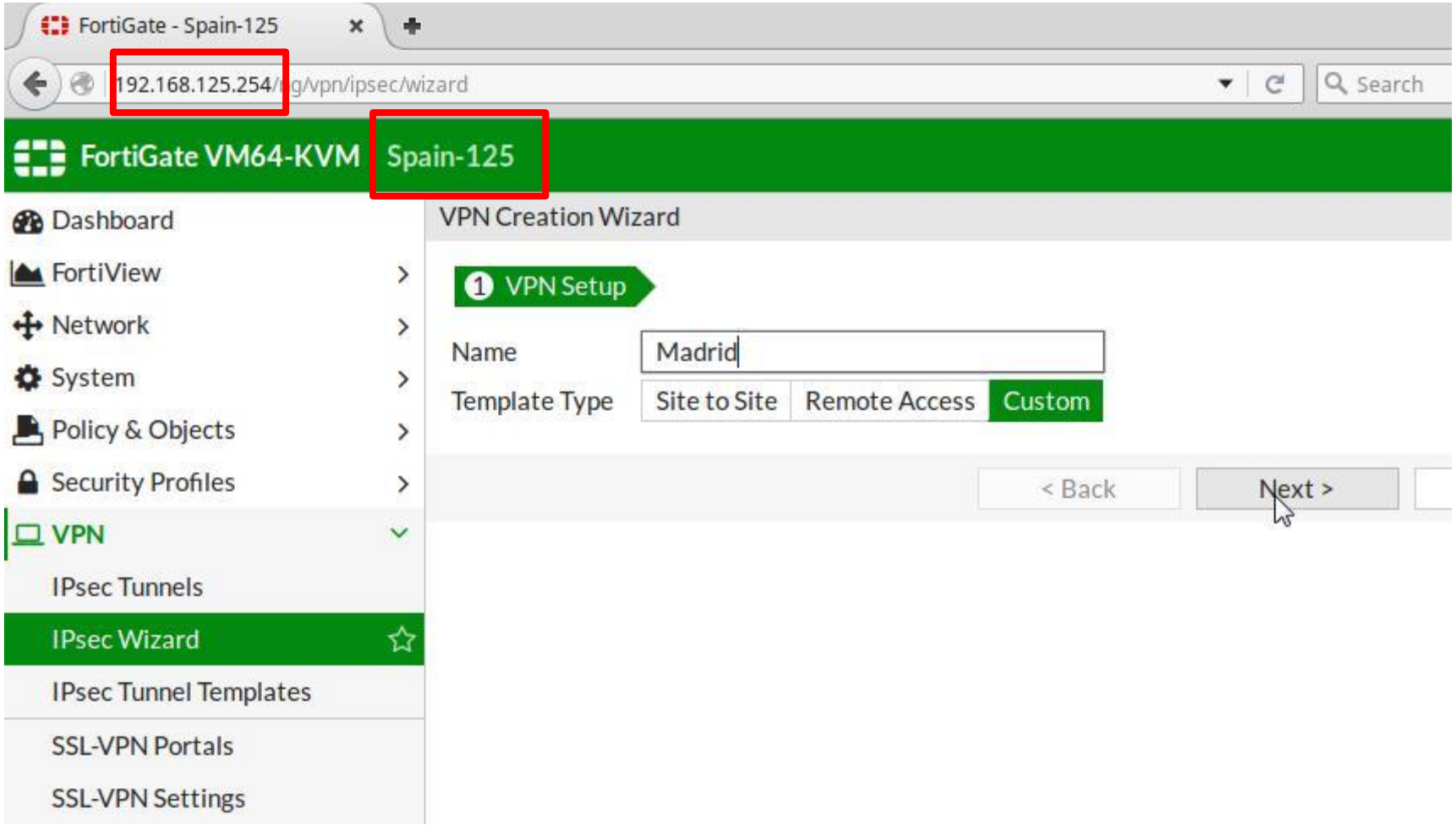
1. Tunnel to the Hub:

   . From the FGT-VM Ping the Hub's overlay IP
   . From the Linux-VM Ping the Hub's server

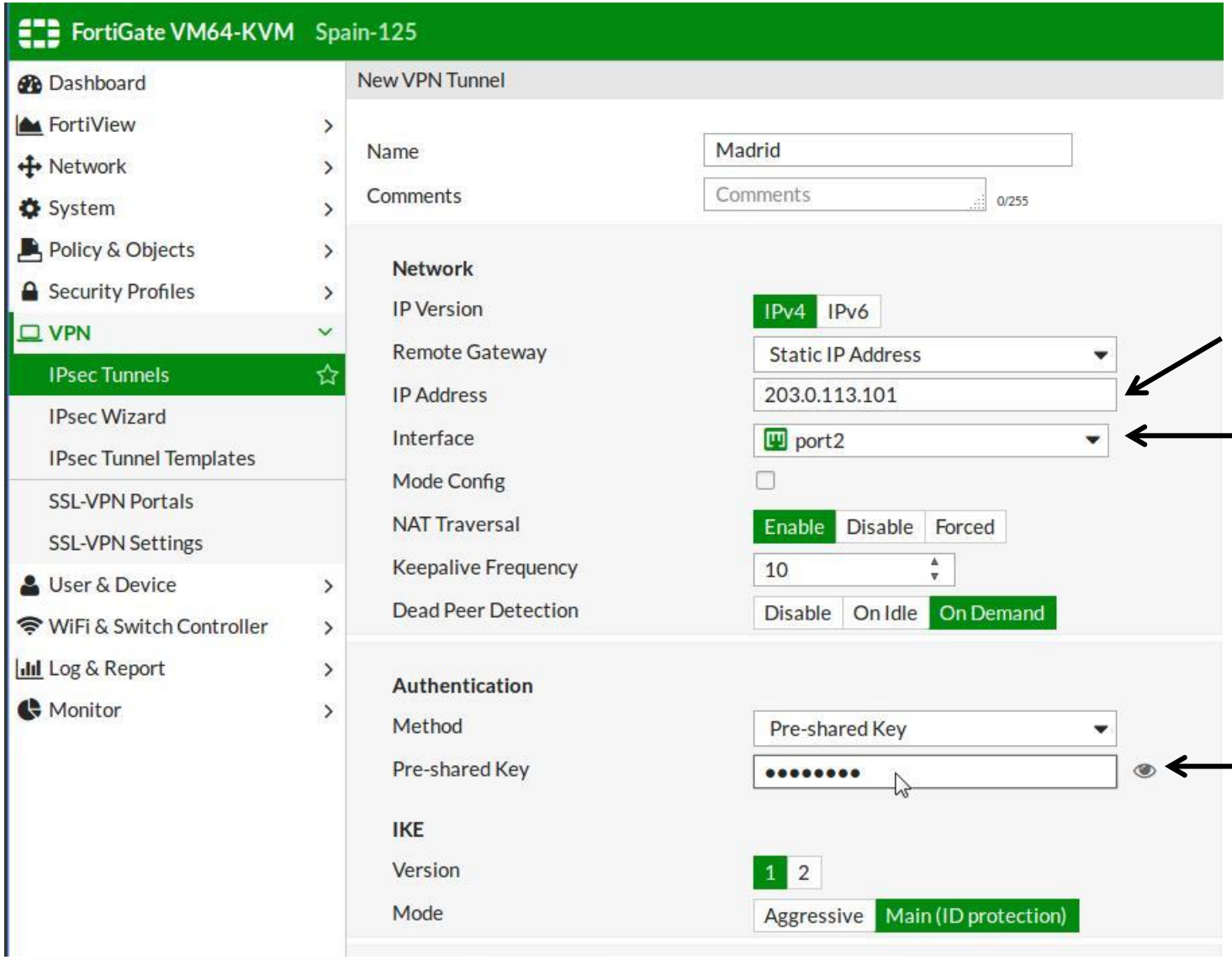
2. Shortcuts:

   . Enable IKE debug
   . From the Linux-VM Ping resources behind other Spokes
   . Check the IKE shortcut negotiation
   . Check the tunnels
   . Check the routing

Config Step 1: Create the tunnel [1/4]



Config Step 1: Create the tunnel [2/4]

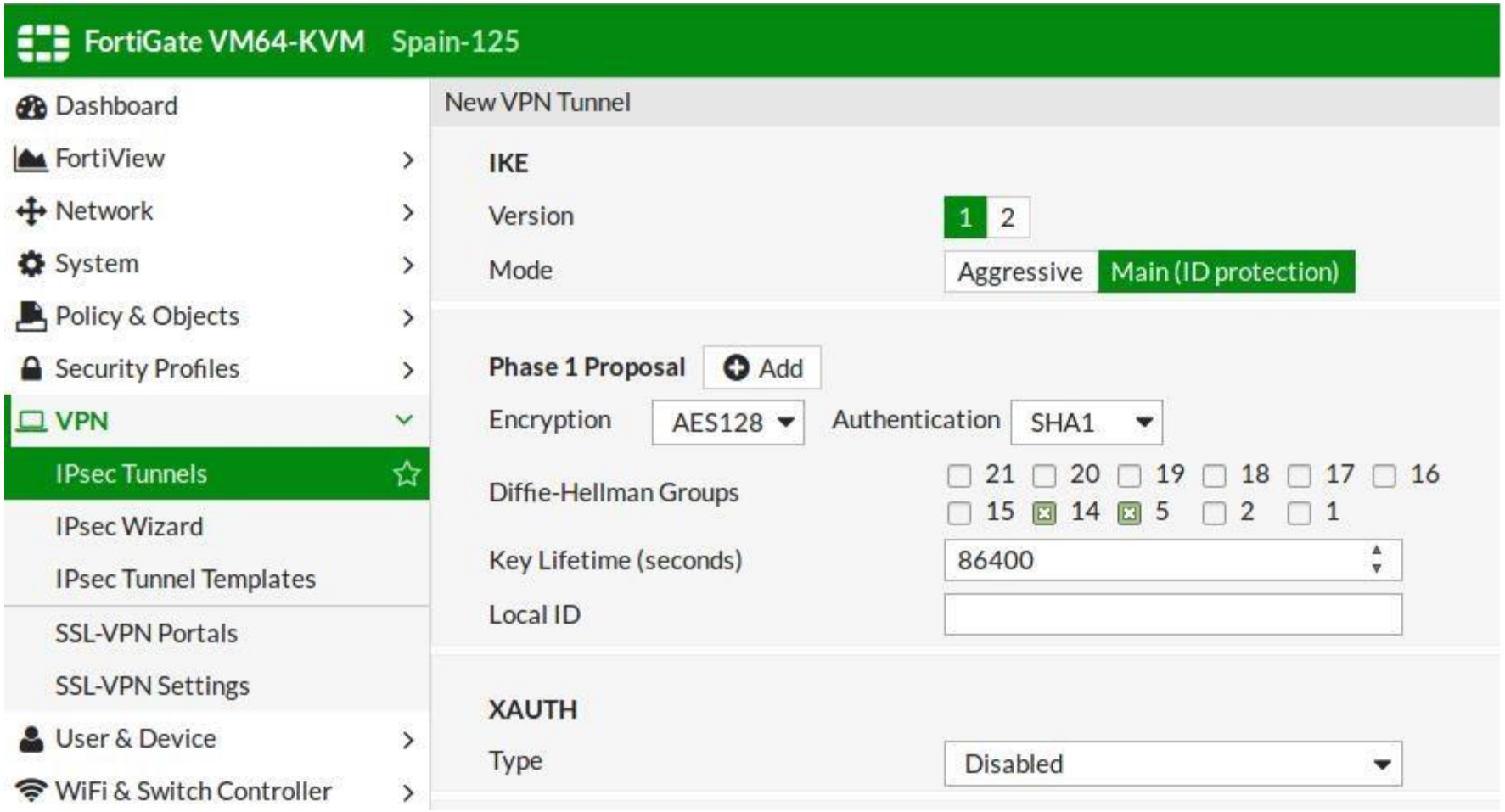


Madrid = 203.0.113.101
Paris = 198.51.100.1

"Internet" interface of the FGT-VM

PSK = fortinet

Config Step 1: Create the tunnel [3/4]



Config Step 1: Create the tunnel [4/4]

FortiGate VM64-KVM Spain-125

- Dashboard
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
  - IPsec Tunnels
  - IPsec Wizard
  - IPsec Tunnel Templates
  - SSL-VPN Portals
  - SSL-VPN Settings
- User & Device
- WiFi & Switch Controller
- Log & Report
- Monitor

New VPN Tunnel

Phase 2 Selectors

Name	Local Address	Remote Address
Madrid	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

New Phase 2

Name	Madrid
Comments	Comments
Local Address	Subnet 0.0.0.0/0.0.0.0
Remote Address	Subnet 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal Add

Encryption AES128 Authentication SHA1

Enable Replay Detection

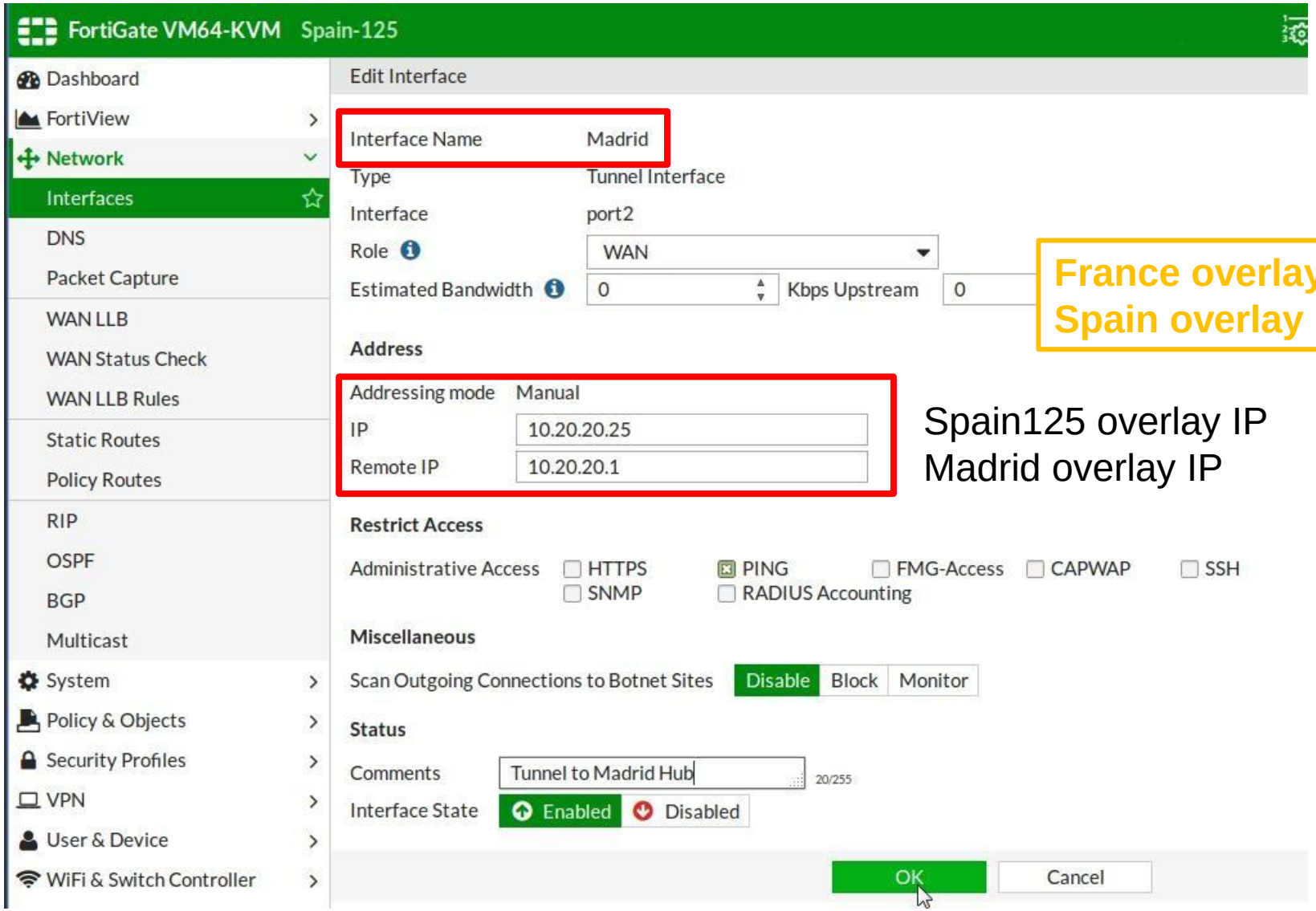
Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group: 21 20 19 18 17 16 15 14 5 2 1

Local Port	All
Remote Port	All
Protocol	All
Auto-negotiate	
Autokey Keep Alive	
Key Lifetime	Seconds
Seconds	43200

OK Cancel

Config Step 2: Overlay IP on the tunnel interface



France overlay = 10.10.10.0/24
Spain overlay = 10.20.20.0/24

Spain125 overlay IP
Madrid overlay IP

Config Step 3: Enable ADVPN on the tunnel

```
Spain-125 #
Spain-125 # config vpn ipsec phase1-interface

Spain-125 (phase1-interface) # edit Madrid

Spain-125 (Madrid) #
Spain-125 (Madrid) # set auto-discovery-receiver enable

Spain-125 (Madrid) #
Spain-125 (Madrid) # end

Spain-125 #
Spain-125 #
```

Config Step 4 & 5: Firewall policies and Overlay routes

4

FortiGate VM64-KVM Spain-125 admin

Dashboard
FortiView
Network
System
Policy & Objects
IPv4 Policy

Create New | Edit | Delete | Policy Lookup | Search | Interface Pair View | By Sequence

Seq.#	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Secur
1	to ADVPN	LAN (port1)	Madrid	all	all	always	ALL	ACCEPT	Disabled	
2	from ADVPN	Madrid	LAN (port1)	all	all	always	ALL	ACCEPT	Disabled	
3	Implicit Deny	any	any	all	all	always	ALL	DENY		

5

FortiGate VM64-KVM Spain-125

Dashboard
FortiView
Network
Interfaces
DNS
Packet Capture
WAN LLB
WAN Status Check
WAN LLB Rules
Static Routes
Policy Routes

Create New | Edit | Clone | Delete

Destination	Gateway	Interface	Comment
0.0.0.0/0	203.0.113.254	port2	
10.20.20.0/24		Madrid	Spain overlay subnet
10.10.10.0/24		Madrid	France overlay subnet
10.255.255.0/30		Madrid	Paris-Madrid overlay

Config Step 6: Configure BGP

France = AS 65000
Spain = AS 65100

FortiGate VM64-KVM Spain-125 admin

- Dashboard
- FortiView
- Network
  - Interfaces
  - DNS
  - Packet Capture
  - WAN LLB
  - WAN Status Check
  - WAN LLB Rules
  - Static Routes
  - Policy Routes
  - RIP
  - OSPF
  - BGP
  - Multicast

Local As: 65100 (1-4294967295)
Router ID: 10.20.20.25 (IP)
Apply

Neighbors IP: Remote As: Add / Edit

Delete

	Neighbor	Remote As
	10.20.20.1	65100

Networks IP/Netmask: Add

Delete

	Network
	192.168.125.0/255.255.255.0

Config: Spoke “Spain125”

Tunnel:

```
config vpn ipsec phase1-interface
    edit "Madrid"
        set interface "port2"
        set proposal aes128-sha1
        set auto-discovery-receiver enable
        set remote-gw 203.0.113.101
        set psksecret fortinet
    next
end

config vpn ipsec phase2-interface
    edit "Madrid"
        set phase1name "Madrid"
        set proposal aes128-sha1
    next
end
```

Interfaces:

```
config system interface
    edit "Madrid"
        set ip 10.20.20.25 255.255.255.255
        set allowaccess ping
        set remote-ip 10.20.20.1
    next
    edit "port1"
        set vdom "root"
        set ip 192.168.125.254 255.255.255.0
        set allowaccess ping https ssh http telnet
        set alias "LAN"
    next
    edit "port2"
        set ip 203.0.113.125 255.255.255.0
        set allowaccess ping
        set alias "ISP2"
    next
end
```

Policies:

```
config firewall policy
    edit 1
        set name "to ADVPN"
        set srcintf "port1"
        set dstintf "Madrid"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "from ADVPN"
        set srcintf "Madrid"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

Config: Spoke “Spain125”

Overlay routes:

```
config router static
    edit 1
        set gateway 203.0.113.254
        set device "port2"
    next
    edit 2
        set dst 10.20.20.0 255.255.255.0
        set device "Madrid"
        set comment "Spain overlay subnet"
    next
    edit 3
        set dst 10.10.10.0 255.255.255.0
        set device "Madrid"
        set comment "France overlay subnet"
    next
    edit 4
        set dst 10.255.255.0 255.255.255.252
        set device "Madrid"
        set comment "Paris-Madrid overlay"
    next
end
```

BGP:

```
config router bgp
    set as 65100
    set router-id 10.20.20.25
    config neighbor
        edit "10.20.20.1"
            set remote-as 65100
        next
    end
    config network
        edit 1
            set prefix 192.168.125.0 255.255.255.0
        next
    end
end
```

Validation Step 1: Tunnel towards the Hub

```
Spain-125 # exec ping 10.20.20.1
PING 10.20.20.1 (10.20.20.1): 56 data bytes
64 bytes from 10.20.20.1: icmp_seq=0 ttl=255 time=0.6 ms
64 bytes from 10.20.20.1: icmp_seq=1 ttl=255 time=0.4 ms
64 bytes from 10.20.20.1: icmp_seq=2 ttl=255 time=0.4 ms
64 bytes from 10.20.20.1: icmp_seq=3 ttl=255 time=0.4 ms
64 bytes from 10.20.20.1: icmp_seq=4 ttl=255 time=0.4 ms

--- 10.20.20.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.4/0.6 ms
```

From the FGT-VM Ping the Hub's overlay IP

Paris overlay IP = 10.10.10.1
Madrid overlay IP = 10.20.20.1

From the Linux-VM Ping the Hub's server

Paris server = 192.168.1.1
Madrid server = 192.168.101.1

```
mint@mint ~ $ ping 192.168.101.1
PING 192.168.101.1 (192.168.101.1): 56 data bytes
64 bytes from 192.168.101.1: icmp_seq=0 ttl=253 time=0.7 ms
64 bytes from 192.168.101.1: icmp_seq=1 ttl=253 time=0.6 ms
64 bytes from 192.168.101.1: icmp_seq=2 ttl=253 time=0.5 ms
64 bytes from 192.168.101.1: icmp_seq=3 ttl=253 time=0.6 ms
64 bytes from 192.168.101.1: icmp_seq=4 ttl=253 time=0.5 ms

--- 192.168.101.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.6/0.7 ms
```

Validation Step 2: Shortcuts

```
Spain-125 # diag debug console timestamp enable
Spain-125 # diag vpn ike log filter clear
Spain-125 # diag debug application ike -1
Spain-125 # diag debug enable
```

Start IKE debug
(don't use any filter so that you can witness all IKE negotiations with the Hub and all the other Spokes)

From the Linux-VM (here, Spain125)
Ping the Linux-VM of another Spoke (here, France02)

```
mint@mint ~ $ ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1): 56 data bytes
64 bytes from 192.168.2.1: icmp_seq=0 ttl=251 time=1.8 ms
64 bytes from 192.168.2.1: icmp_seq=1 ttl=253 time=0.7 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=253 time=0.7 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=253 time=0.8 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=253 time=0.7 ms

--- 192.168.2.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.7/0.9/1.8 ms
```

Validation Step 2: Shortcuts

IKE Shortcut negotiation between Spain102 and France02:

```
ike 0: comes 203.0.113.1:500->203.0.113.125:500,ifindex=4....
ike 0: IKEv1 exchange=Informational id=8b0f747cb261ee48/965a8ff8f3cd8b12:75dcd867 len=172
ike 0:Madrid:39: notify msg received: SHORTCUT-OFFER
ike 0:Madrid: shortcut-offer 192.168.125.1->192.168.2.1 psk 64
```

Shortcut-offer received from the Hub

```
ike 0:Madrid:39: sent IKE msg (SHORTCUT-QUERY): 203.0.113.125:500->203.0.113.1:500, len=204, id=8b0f747cb261ee48/965a8ff8f3cd8b12:4ac6f02e
```

Shortcut-query sent to France02 via the Hub

```
ike 0: comes 203.0.113.1:500->203.0.113.125:500,ifindex=4....
ike 0: IKEv1 exchange=Informational id=8b0f747cb261ee48/965a8ff8f3cd8b12:11a2754f len=188
ike 0:Madrid:39: notify msg received: SHORTCUT-REPLY
ike 0:Madrid: recv shortcut-reply 14169010131944755998 a0862cdd0191a334/7f408cabf9c1a64e 198.51.100.2 to 192.168.125.1 psk 64
ike 0:Madrid: shortcut-reply route to 192.168.125.1 via root 13
```

Shortcut-reply received from France02 via the Hub

```
ike 0:Madrid: created connection: 0x6e35e00 4 203.0.113.125->198.51.100.2:500.
ike 0:Madrid: adding new dynamic tunnel for 198.51.100.2:500
ike 0:Madrid_0: added new dynamic tunnel for 198.51.100.2:500
ike 0:Madrid_0:41: initiator: main mode is sending 1st message...
ike 0:Madrid_0:41: cookie a0862cdd0191a334/7f408cabf9c1a64e
ike 0:Madrid_0:41: sent IKE msg (ident_i1send): 203.0.113.125:500->198.51.100.2:500, len=372, id=a0862cdd0191a334/7f408cabf9c1a64e
...
...
...
```

Shortcut ‘Madrid_0’ is created and IKE negotiation with France02 is starting…

FORTINET®

FORTINET XPERTS ACADEMY